Forensic Toolkit (FTK)

User Guide

ACCESSDATA®

AccessData Legal and Contact Information

Document date: April 3, 2017

Legal Information

©2017 AccessData Group, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

AccessData Group, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, AccessData Group, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, AccessData Group, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, AccessData Group, Inc. reserves the right to make changes to any and all parts of AccessData software, at any time, without any obligation to notify any person or entity of such changes.

You may not export or re-export this product in violation of any applicable laws or regulations including, without limitation, U.S. export regulations or the laws of the country in which you reside.

AccessData Group, Inc.
588 West 400 South Suite 350
Lindon, UT 84042
USA

AccessData Trademarks and Copyright Information

The following are either registered trademarks or trademarks of AccessData Group, Inc. All other trademarks are the property of their respective owners.

AccessData®	DNA®	PRTK®
AccessData Certified Examiner® (ACE®)	Forensic Toolkit® (FTK®)	Registry Viewer®
AD Summation®	Mobile Phone Examiner Plus®	Summation®
Discovery Cracker®	MPE+ Velocitor™	SilentRunner®
Distributed Network Attack®	Password Recovery Toolkit®	

A trademark symbol (®, ™, etc.) denotes an AccessData Group, Inc. trademark. With few exceptions, and unless otherwise notated, all third-party product names are spelled and capitalized the same way the owner spells and capitalizes its product name. Third-party trademarks and copyrights are the property of the trademark and copyright holders. AccessData claims no responsibility for the function or performance of third-party products.

Third party acknowledgements:

- FreeBSD ® Copyright 1992-2011. The FreeBSD Project.
- AFF® and AFFLIB® Copyright® 2005, 2006, 2007, 2008 Simson L. Garfinkel and Basis Technology Corp. All rights reserved.
- Copyright © 2005 - 2009 Ayende Rahien

BSD License:
Copyright (c) 2009-2011, Andriy Syrov. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer; Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution; Neither the name of Andriy Syrov nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

WordNet License:
This license is available as the file LICENSE in any downloaded version of WordNet.
WordNet 3.0 license: (Download)
WordNet Release 3.0 This software and database is being provided to you, the LICENSEE, by Princeton University under the following license. By obtaining, using and/or copying this software and database, you agree that you have read, understood, and will comply with these terms and conditions.: Permission to use, copy, modify and distribute this software and database and its documentation for any purpose and without fee or royalty is hereby granted, provided that you agree to comply with the following copyright notice and statements, including the disclaimer, and that the same appear on ALL copies of the software, database and documentation, including modifications that you make for internal use or for distribution. WordNet 3.0 Copyright 2006 by Princeton University. All rights reserved. THIS SOFTWARE AND DATABASE IS PROVIDED "AS IS" AND PRINCETON UNIVERSITY MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PRINCETON UNIVERSITY MAKES NO REPRESENTATIONS OR WARRANTIES OF MERCHANT- ABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE LICENSED SOFTWARE, DATABASE OR DOCUMENTATION WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. The name of Princeton University or Princeton may not be used in advertising or publicity pertaining to distribution of the software and/or database.

Title to copyright in this software, database and any associated documentation shall at all times remain with Princeton University and LICENSEE agrees to preserve same.

XMLmind XSL-FO Converter Professional Edition Developer License Agreement:
Distribution
Licensee may not distribute with the Application any component of the Software other than the binary class library (xfc.jar) for the JavaTM version and the Dynamic Link Library file (xfc.dll) for the .NET version.
Licensee shall include the following copyright notice: "XMLmind XSL-FO Converter Copyright © 2002-2009 Pixware SARL", with every copy of the Application. This copyright notice may be placed together with Licensee's own copyright notices, or in any reasonably visible location in the packaging or documentation of the Application.
Licensee may use, distribute, license and sell the Application without additional fees due to Licensor, subject to all the conditions of this License Agreement.

Documentation Conventions

In AccessData documentation, a number of text variations are used to indicate meanings or actions. For example, a greater-than symbol (>) is used to separate actions within a step. Where an entry must be typed in using the keyboard, the variable data is set apart using [*variable_data*] format. Steps that require the user to click on a button or icon are indicated by **Bolded text**. This *Italic* font indicates a label or non-interactive item in the user interface.

A trademark symbol (®, ™, etc.) denotes an AccessData Group, Inc. trademark. Unless otherwise notated, all third-party product names are spelled and capitalized the same way the owner spells and capitalizes its product name. Third-party trademarks and copyrights are the property of the trademark and copyright holders. AccessData claims no responsibility for the function or performance of third-party products.

Registration

The AccessData product registration is done at AccessData after a purchase is made, and before the product is shipped. The licenses are bound to either a USB security device, or a Virtual CmStick, according to your purchase.

Subscriptions

AccessData provides a one-year licensing subscription with all new product purchases. The subscription allows you to access technical support, and to download and install the latest releases for your licensed products during the active license period.

Following the initial licensing period, a subscription renewal is required annually for continued support and for updating your products. You can renew your subscriptions through your AccessData Sales Representative.

Use License Manager to view your current registration information, to check for product updates and to download the latest product versions, where they are available for download. You can also visit our web site,

www.accessdata.com anytime to find the latest releases of our products.

For more information, see Managing Licenses in your product manual or on the AccessData website.

AccessData Contact Information

Your AccessData Sales Representative is your main contact with AccessData. Also, listed below are the general AccessData telephone number and mailing address, and telephone numbers for contacting individual departments

Mailing Address and General Phone Numbers

You can contact AccessData in the following ways:

AccessData Mailing Address, Hours, and Department Phone Numbers

Corporate Headquarters:	AccessData Group, Inc. 588 West 400 South Suite 350 Lindon, UT 84042 USA *Voice*: 801.377.5410; *Fax*: 801.377.5426
General Corporate Hours:	Monday through Friday, 8:00 AM – 5:00 PM (MST) AccessData is closed on US Federal Holidays
State and Local Law Enforcement Sales:	*Voice*: 800.574.5199, option 1; *Fax*: 801.765.4370 *Email*: Sales@AccessData.com
Federal Sales:	*Voice*: 800.574.5199, option 2; *Fax*: 801.765.4370 *Email*: Sales@AccessData.com
Corporate Sales:	*Voice*: 801.377.5410, option 3; *Fax*: 801.765.4370 *Email*: Sales@AccessData.com
Training:	*Voice*: 801.377.5410, option 6; *Fax*: 801.765.4370 *Email*: Training@AccessData.com
Accounting:	*Voice*: 801.377.5410, option 4

Technical Support

Technical support is available on all currently licensed AccessData solutions.
You can contact AccessData Customer and Technical Support in the following ways:

AccessData Support Portal

You can access the Chat, Knowledge Base, Discussion Boards, White Papers and more through the AccessData Support Portal:

https://support.accessdata.com

E-Mail Support:

support@accessdata.com

Telephone:

Americas/Asia-Pacific:

800-658-5199 (North America)

Support Hours: Mon-Fri, 7:00 AM – 6:00 PM (MST), except corporate holidays.

NOTE: Emergency support is available on weekends:

Saturday and Sunday 8:00am – 6:00pm MST via support@accessdata.com

Documentation

Please email AccessData regarding any typos, inaccuracies, or other problems you find with the documentation: *documentation@accessdata.com*

Professional Services

The AccessData Professional Services staff comes with a varied and extensive background in digital investigations including law enforcement, counter-intelligence, and corporate security. Their collective experience in working with both government and commercial entities, as well as in providing expert testimony, enables them to provide a full range of computer forensic and eDiscovery services.

At this time, Professional Services provides support for sales, installation, training, and utilization of Summation, FTK, FTK Pro, Enterprise, eDiscovery, Lab and the entire Resolution One platform. They can help you resolve any questions or problems you may have regarding these solutions.

Contact Information for Professional Services

Contact AccessData Professional Services in the following ways:

AccessData Professional Services Contact Information

Contact Method	Number or Address
Phone	North America Toll Free: 800-489-5199, option 7
	International: +1.801.377.5410, option 7
Email	*services@accessdata.com*

Table of Contents

AccessData Legal and Contact Information 2

Table of Contents 7

Part 1: Introducing Forensic Toolkit® (FTK®) 24

Chapter 1: Introducing AccessData® Forensic Toolkit® (FTK®) 25

Overview of Investigating Digital Evidence 25
About Acquiring Digital Evidence 26
Types of Digital Evidence 26
Acquiring Evidence 26
About Examining Digital Evidence 27
About Managing Cases and Evidence 28
What You Can Do With the Examiner 29
About Indexing and Hashing 29
About the Known File Filter Database 29
About Searching 30
About Bookmarking 30
About Presenting Evidence 30

Chapter 2: Getting Started with the User Interface 31

Part 2: Administrating Forensic Toolkit® (FTK®) 33

Chapter 3: Application Administration 34

Initializing the Database and Creating an Application Administrator Account . . . 35
Changing Your Password 36
Recovering a Password 36
Creating a Password Reset File 36
Resetting your Password 37
Setting Database Preferences 38
Managing Database Sessions 38
Optimizing the Database for Large Cases 38
Creating Databases for Individual Cases 39
Managing KFF Settings 39
Recovering and Deleting Processing Jobs 40
Restoring an Image to a Disk 40

Database Integration with other AccessData Products 41
Web Viewer 41
Adding New Users to a Database 42
About Assigning Roles to Users 42
About Additional Roles 43
About Predefined Roles 43
Assigning Initial Database-level Roles to Users 46
Assigning Additional Case-level Roles to Users 46
Assigning Users Shared Label Visibility 47
Setting Additional Preferences 47
Choosing a Temporary File Path 47
Providing a Network Security Device Location 47
Setting Theme Preferences for the Visualization Add on 48
Optimizing the Case Database 48
Managing Global Features 48
Managing Shared Custom Carvers 48
Managing Custom Identifiers 49
Managing Columns 50
Managing File Extension Maps 50
Managing Filters 51

Part 3: Case Management 52

Chapter 4: Introducing Case Management 53
About Case Management 53
The User Interfaces 53
About the Cases List 54
Menus of the Case Manager 55
Menus of the Examiner 61

Chapter 5: Creating and Configuring New Cases 73
Opening an Existing Case 73
Creating a Case 74
Configuring Detailed Options for a Case 75
About Processing Options 75
Configuring Default Processing Options for a Case 76
Using Processing Profiles 77
Manually Customizing a set of Detailed Options 81
Evidence Processing Options 82
Expanding Compound Files 85
Using dtSearch Text Indexing 88
Configuring Case Indexing Options 88
Data Carving 91

Running Optical Character Recognition (OCR) 95
Using Explicit Image Detection 96
Including Registry Reports 97
Send Email Alert on Job Completion 98
Custom File Identification Options 98
Creating Custom File Identifiers 98
Configuring Evidence Refinement (Advanced) Options 100
Refining Evidence by File Status/Type 101
Selecting Index Refinement (Advanced) Options 102
Selecting Lab/eDiscovery Options 104
Adding Evidence to a New Case 107
Working with Volume Shadow Copies 107
Converting a Case from Version 2.2 or Newer 107

Chapter 6: Managing Case Data 108
Backing Up a Case 109
About Performing a Backup and Restore on a Multi-Box Installation 109
Performing a Backup of a Case 109
Performing a Database-only Backup 110
Archiving a Case 111
Archiving and Detaching a Case 112
Attaching a Case 113
Restoring a Case 114
Deleting a Case 115
Storing Case Files 115
Migrating Cases Between Database Types 115

Chapter 7: Working with Evidence Image Files 117
Verifying Drive Image Integrity 117
Mounting an Image to a Drive 118
Benefits of Image Mounting 118
Characteristics of a Logically Mounted Image 119
Characteristics of a Physically Mounted Image 119
Mounting an Image as Read-Only 119
Mounting a Drive Image as Writable 120
Unmounting an Image 121
Restoring an Image to a Disk 121
Performing Final Carve Processing 121
Recovering Processing Jobs 122

Chapter 8: Working with Static Evidence 123
Static Evidence Compared to Remote Evidence 123

Acquiring and Preserving Static Evidence . . . 124
Adding Evidence . . . 124
Working with Evidence Groups . . . 128
Selecting Evidence Processing Options . . . 129
Selecting a Language . . . 130
Examining Data in Volume Shadow Copies . . . 131
About Restore Point Processing Options . . . 132
Managing Restore Points . . . 133
Viewing Restore Point Data . . . 133
Using Additional Analysis . . . 135
Hashing . . . 140
Data Carving . . . 140
Viewing the Status and Progress of Data Processing and Analysis . . . 142
Viewing Processed Items . . . 143

Chapter 9: Working with Live Evidence . . . 144
About Live Evidence . . . 144
Types of Live Evidence . . . 145
Adding Local Live Evidence . . . 145
Methods of Adding Remote Live Evidence . . . 146
Requirements for Adding Remote Live Evidence . . . 146
Adding Evidence with the Temporary Agent . . . 147
Pushing the Temporary Agent . . . 147
Manually Deploying the Temporary Agent . . . 148
Adding Data with the Enterprise Agent . . . 149
Methods of Deploying the Enterprise Agent . . . 149
Creating Self-signed Certificates for Agent Deployment . . . 149
Configuring Communication Settings for the Enterprise Agent Push . . . 150
Pushing the Enterprise Agent . . . 151
Removing the Enterprise Agent . . . 152
Connecting to an Enterprise Agent . . . 152
Adding Remote Data with the Enterprise Agent . . . 152
Acquiring Drive Data . . . 155
Acquiring RAM Data . . . 156
Importing Memory Dumps . . . 157
Unmounting an Agent Drive or Device . . . 157

Chapter 10: Filtering Data to Locate Evidence . . . 158
About Filtering . . . 158
Types of Filters . . . 159
What You Can Do with Filters . . . 159
Understanding How Filters Work . . . 161
Viewing the Components of Filters . . . 161

Viewing Details about Attributes that Filters use . . . 161
Using Simple Filtering . . . 162
Using Global Filters . . . 162
Using Tab Filters . . . 162
How Global Filters and Tab Filters can work Together . . . 163
Using Filters with Category Containers . . . 163
Using Filters with Reports . . . 163
Viewing the Filters that you have Applied . . . 164
Using Filtering with Searches . . . 165
Adding a Search Filter to Live Searches . . . 165
Adding a Search Filter to Index Searches . . . 165
Using Compound Filters . . . 166
Applying Compound Filters . . . 166
Using Custom Filters . . . 167
About Nested Filters . . . 167
Creating a Custom Filter . . . 167
Copying Filters . . . 168
Editing a Custom Filter . . . 168
Sharing, Importing, and Exporting Filters . . . 169
Sharing Custom Filters Between Cases . . . 169
Importing Filters . . . 169
Exporting Filters . . . 169
Types of Predefined Filters . . . 170
Using the Persons of Interest Filter . . . 174
Creating a List of Communication Participants . . . 174
Creating a Rule within People Finder . . . 175
Searching for Data within People Finder . . . 175
Creating a Communication Filter within People Finder . . . 175
Fields Searched when using Persons of Interest . . . 176

Chapter 11: Working with Labels . . . 177
What You Can Do With Labels . . . 177
Creating a Label . . . 178
Applying a Label . . . 178
Managing Labels . . . 179
Managing Label Groups . . . 180

Chapter 12: Decrypting Files . . . 181
About Decrypting Files . . . 181
About the Encrypted File Passwords List . . . 183
Identifying the Encrypted Files in a Case . . . 185
Using PRTK/DNA Integration . . . 186
Decrypting Files Using the Automatic Decryption Processing Option . . . 186

Decrypting Files Using Right-Click Auto Decryption . . . 187
Recovering Unknown Passwords of Encrypted Files . . . 188
About Recovering Passwords using the PRTK/DNA Integrated Tool with Examiner 188
Recovering Passwords using the PRTK/DNA Integrated Tool . . . 188
Decrypting Other Encryption Types . . . 190
Decrypting EFS . . . 190
Decrypting Microsoft Office Digital Rights Management (DRM) Protected Files 191
Decrypting Dropbox DBX Files . . . 192
Decrypting Lotus Notes Files . . . 193
Decrypting S/MIME Files . . . 193
Decrypting Credant Files (Dell Data Protection | Encryption Server) . . . 194
Decrypting Bitlocker Partitions . . . 196
Decrypting Safeguard Utimaco Files . . . 197
Decrypting SafeBoot Files . . . 199
Decrypting Guardian Edge Files . . . 199
Decrypting an Image Encrypted With PGP® WDE . . . 199
Viewing Decrypted Files . . . 201

Chapter 13: Exporting Data from the Examiner . . . 202
Copying Information from the Examiner . . . 202
Exporting Files to a Native Format . . . 204
Exporting Files to an AD1 Image . . . 206
Exporting an Image to an Image . . . 208
Exporting File List Information . . . 210
Exporting a Word List . . . 211
Exporting Recycle Bin Index Contents . . . 211
Exporting Hashes from a Case . . . 212
Exporting KFF Data . . . 212
Exporting All Hits in a Search to a CSV file . . . 213
Exporting Emails to PST . . . 214
Exporting the Properties Panel . . . 215
Exporting Geolocation Data to KML or KMZ . . . 216

Chapter 14: About Cerberus Malware Analysis . . . 217
About Cerberus Malware Analysis . . . 217
About Cerberus Stage 1 Threat Analysis . . . 218
About Cerberus Score Weighting . . . 218
About Cerberus Override Scores . . . 218
About Cerberus Threat Score Reports . . . 219
Cerberus Stage 1 Threat Scores . . . 221
Cerberus Stage 1 File Information . . . 223

About Cerberus Stage 2 Static Analysis . . . 224
About Cerberus Stage 2 Report Data . . . 224
Cerberus Stage 2 Function Call Data . . . 225
File Access Call Categories . . . 226
Networking Functionality Call Categories . . . 228
Process Manipulation Call Categories . . . 230
Security Access Call Categories . . . 231
Windows Registry Call Categories . . . 231
Surveillance Call Categories . . . 232
Uses Cryptography Call Categories . . . 232
Low-level Access Call Categories . . . 233
Loads a driver Call Categories . . . 233
Subverts API Call Categories . . . 234

Chapter 15: Running Cerberus Malware Analysis . . . 235
Running Cerberus Analysis . . . 235
About Reviewing Results of Cerberus . . . 237
Cerberus Columns . . . 237
Reviewing Results of Cerberus . . . 239
Using Index Search with Cerberus . . . 240
Exporting a Cerberus Report . . . 240

Chapter 16: Using the Known File Filter (KFF) . . . 241
Process for Using KFF . . . 241
About the KFF Admin page . . . 242
Adding Hashes to the KFF Server . . . 244
Importing KFF Data . . . 244
Manually Managing Hashes in a Hash Set . . . 246
Adding Hashes From Files in Cases . . . 247
Using KFF Groups to Organize Hash Sets . . . 248
About KFF Groups . . . 248
Creating a KFF Group . . . 249
Viewing the Contents of a KFF Group . . . 249
Managing KFF Groups . . . 249
Enabling a Case to Use KFF . . . 251
About Enabling and Configuring KFF . . . 251
Enabling and Configuring KFF . . . 251
Reviewing KFF Results in the Examiner . . . 253
About KFF Data Shown in the Item List . . . 253
Using the KFF Information Columns . . . 253
Using KFF Filters . . . 254
Using the Overview Tab . . . 254

Re-Processing KFF Using Additional Analysis . . . 255
Exporting KFF Data . . . 256
About Exporting KFF Data . . . 256
Exporting KFF Groups . . . 256
Archiving the KFF Server's Data . . . 256

Chapter 17: Getting Started with KFF (Known File Filter) . . . 257
About KFF . . . 257
Introduction to the KFF Architecture . . . 258
Components of KFF Data . . . 258
How KFF Works . . . 260
About the KFF Server and Geolocation . . . 262
Installing the KFF Server . . . 263
About Installing the KFF Server . . . 263
About KFF Server Versions . . . 263
Process for Installing KFF . . . 264
Downloading the Latest KFF Installation Files . . . 264
Installing the KFF Server Service . . . 264
Configuring the Location of the KFF Server . . . 265
Configuring the KFF Server Location on FTK-based Applications . . . 265
Configuring the KFF Server Location on eDiscovery . . . 265
Migrating Legacy KFF Data . . . 266
Importing KFF Data . . . 268
About Importing KFF Data . . . 268
Using the KFF Import Utility . . . 269
Importing Pre-defined KFF Data Libraries . . . 271
Installing the Geolocation (GeoIP) Data . . . 274
About CSV and Binary Formats . . . 275
Uninstalling KFF . . . 278
Installing KFF Updates . . . 279
KFF Library Reference Information . . . 280
About KFF Pre-Defined Hash Libraries . . . 280
What has Changed in Version 5.6 . . . 285

Part 4: Reviewing Cases . . . 286

Chapter 18: Using the Examiner Interface . . . 287
About the Examiner . . . 287
Creating Screen Captures in the Examiner . . . 288

Chapter 19: Exploring Evidence . . . 289
Explorer Tree Pane . . . 289

File List Pane . . . 290
Using the File List's Columns . . . 290
Icons of the File List Tool Bar . . . 292
File List View Right-Click Menu . . . 294
The File Content Viewer Pane . . . 296
The Filter Toolbar . . . 304
Using QuickPicks . . . 305

Chapter 20: Examining Evidence in the Overview Tab . . . 306
Using the Overview Tab . . . 306
Evidence Groups Container . . . 306
File Items Container . . . 306
File Extension Container . . . 307
File Category Container . . . 307
File Status Container . . . 308
Cluster Topic Container . . . 309
Processing and Displaying Evidence Counts . . . 309
Disabling the Calculation and Display of the Total Logical Size . . . 310

Chapter 21: Examining Email . . . 311
Using the Email Tab . . . 311
Email Status Tree . . . 311
Email Archives Tree . . . 312
Email Tree . . . 312
Examining Windows 10 Email . . . 313
Processing Windows 10 Email and Contacts . . . 313
Viewing Windows 10 Email and Contacts . . . 313
Exporting Windows 10 Email . . . 314

Chapter 22: Examining Graphics . . . 315
Using the Graphics Tab . . . 315
The Thumbnails Size Setting . . . 316
Moving the Thumbnails Pane . . . 317
Evaluating Explicit Material . . . 319
Filtering EID Material . . . 319
EID Scoring . . . 320
Using PhotoDNA to Compare Images . . . 322
About Using PhotoDNA . . . 322
About the PhotoDNA Library Management Page . . . 322
About the PhotoDNA Processing Option . . . 322
About viewing the PhotoDNA results . . . 323
Configuring a PhotoDNA Library . . . 323
Comparing Images to the PhotoDNA Library . . . 324

Chapter 23: Examining Videos 326
Generating Thumbnails for Video Files 327
Generating Video Thumbnails from the Natural Viewer 327
Creating Common Video Files 328
Using the Video Tree Pane 329
Using the Video Thumbnails Pane 330
Playing a Video from a Video Thumbnail 330
The Thumbnail Size Setting 331
Moving the Thumbnails Pane 331

Chapter 24: Examining Miscellaneous Evidence 332
Identifying Processing-Generated Data 333
Relating Generated Files to Original Files 333
Viewing Windows Prefetch Data 334
Viewing Data in Windows XML Event Log (EVTX) Files 334
About Viewing EVTX Log Files 334
Viewing IIS Log File Data 336
Viewing Registry Timeline Data 338
Viewing Log2Timeline CSV File Data 340
Identifying Document Languages 343
Examining Internet Artifact Data 345
About Extensible Storage Engine (ESE) Databases 346
About Expanding Google Chrome, Firefox, and IE 9 Data 347
About Expanding Data from Internet Explorer (IE) Version 10 or Later 348
Expanding Internet Artifact Data 350
Viewing Internet Artifact Data 351
Examining Mobile Phone Data 352
About Expanding Mobile Phone Data 353
Viewing Mobile Phone Data 357
Working with Cellebrite UFDR Images 358
Working with iOS Backup 359
Working with Facebook Messenger (Android) 360
Viewing Data in Volume Shadow Copies 361
Viewing Microsoft Office and Adobe Metadata 361
About Windows 8 and 10 Keyword Searches 362

Chapter 25: Bookmarking Evidence 364
About Bookmarks 364
About Timeline Bookmarks 364
Creating a Bookmark 365
About Empty Bookmarks 366

Bookmarks Dialog Options . . . 367
Bookmark Comments HTML Editor . . . 369
Viewing Bookmark Information . . . 371
Creating a Timeline Bookmark Report . . . 371
Using the Bookmarks Tab . . . 371
Bookmarking Selected Text . . . 372
Bookmarking Video Thumbnails . . . 372
Adding a Video Thumbnail to a New or Existing Bookmark . . . 372
Adding to an Existing Bookmark . . . 373
Creating Email or Email Attachment Bookmarks . . . 374
Adding Email and Email Attachments to Existing Bookmarks . . . 374
Moving a Bookmark . . . 375
Copying a Bookmark . . . 375
Deleting a Bookmark . . . 375
Deleting Files from a Bookmark . . . 375

Chapter 26: Searching Evidence with Live Search . . . 376
Conducting a Live Search . . . 376
Live Text Search . . . 377
Live Hex Search . . . 379
Live Pattern Search . . . 380
Using Pattern Searches . . . 380
Predefined Regular Expressions . . . 383
Social Security Number . . . 383
U.S. Phone Number . . . 383
IP Address . . . 384
Creating Custom Regular Expressions . . . 385

Chapter 27: Searching Evidence with Index Search . . . 387
Conducting an Index Search . . . 388
Using Search Terms . . . 389
Using Unicode Characters in Search Terms . . . 389
Expanding Search Terms . . . 389
Defining Search Criteria . . . 391
Exporting and Importing Index Search Terms . . . 391
Selecting Index Search Options . . . 392
Viewing Index Search Results . . . 393
Using dtSearch Regular Expressions . . . 394
TR1 Regular Expressions For Text Patterns . . . 394
TR1 Regular Expressions For Number Patterns . . . 398

Documenting Search Results . . . 400
Using Copy Special to Document Search Results . . . 401
Bookmarking Search Results . . . 402

Chapter 28: Viewing System Information . . . 403
About Viewing System Information . . . 403
Populating the Data in the System Information Tab . . . 404
Viewing System Information . . . 404
Exporting System Information Data . . . 405
Available System Information Data . . . 406

Chapter 29: Examining Volatile Data . . . 411
Using the Volatile Tab . . . 412
Understanding Memory . . . 414
Viewing Memory Dump Data . . . 415
Viewing Hidden Processes . . . 415
Viewing Input/Output Request Packet Data . . . 415
Viewing Virtual Address Descriptor (VAD) Data . . . 415
Performing File Remediation from the Volatile Tab . . . 417
Killing a Process . . . 417
Wiping a File . . . 418
Adding Hashes to KFF Library from the Volatile Tab . . . 418
Adding Hashes to Fuzzy Hash Library from the Volatile Tab . . . 419
Creating a Memory Dump File . . . 419

Chapter 30: Analyzing Document Content . . . 420
Using Entity Extraction . . . 420
About Entity Extraction . . . 420
Enabling Entity Extraction . . . 423
Viewing Entity Extraction Data . . . 423
Using Document Content Analysis . . . 424
Filtering Documents by Document Content Analysis . . . 424
Prerequisites for Cluster Topic . . . 425
How Document Content Analysis Works . . . 425
Filtering with Cluster Topic . . . 425
Considerations of Cluster Topic . . . 425
Performing Cluster Analysis . . . 426
Words Excluded from Cluster Analysis Processing . . . 427

Chapter 31: Using Visualization . . . 428
About Visualization . . . 428

Launching Visualization . . . 429
About the Visualization page . . . 430
About Visualization Time Line Views . . . 431
About the Base Time Line . . . 431
Setting the Base Time Line . . . 433
Changing the View of Visualization . . . 434
Modifying the Bar Chart Displays . . . 434
Changing the Theme of Visualization . . . 434
Visualizing File Data . . . 435
Configuring Visualization File Dates . . . 435
Visualizing File Extension Distribution . . . 436
Visualizing File Category Distribution . . . 437
Using the File Data List . . . 438
Visualizing Email Data . . . 442
Narrowing the Scope with the Email Time Line . . . 442
Viewing Mail Statistics . . . 444
Using the Email Details List . . . 444
About the Detailed Visualization Time Line . . . 448
Using the Detailed Visualization Time Line . . . 449
Understanding How Data is Represented in the Detailed Time Line . . . 449
About Time Bands . . . 450
Modifying the Time Line Using Time Bands and Zoom . . . 452
Understanding How Grouping Works in the Detailed Visualization Time Line . . . 452
Visualizing Internet Browser History Data . . . 454
Visualizing Other Data . . . 454

Chapter 32: Using Visualization Heatmap . . . 455

Chapter 33: Using Visualization Social Analyzer . . . 457
About Social Analyzer . . . 457
Accessing Social Analyzer . . . 459
Social Analyzer Options . . . 460
Analyzing Email Domains in Visualization . . . 461
Analyzing Individual Emails in Visualization . . . 461

Chapter 34: Using Visualization Geolocation . . . 463
About Geolocation Visualization . . . 463
About Viewing Geolocation Data . . . 463
General Geolocation System Requirements . . . 464
Processing Geolocation Data . . . 464
Viewing Geolocation EXIF Data . . . 465
Using Geolocation Tools . . . 466
The Geolocation Map Panel . . . 466

Using the Geolocation Grid . . . 469
Filtering Items in the Geolocation Grid . . . 469
Using Geolocation Columns in the Item List . . . 470
Using Geolocation Column Templates . . . 471
Using Geolocation Facets . . . 471
Using Geolocation Visualization to View Security Data . . . 472
Prerequisites for Using Geolocation Visualization to View Security Data . . . 472
Configuring the Geolocation Location Configuration File . . . 472
Viewing Geolocation IP Locations Data . . . 474
Using the Geolocation Network Information Grid . . . 475
Geolocation Filter . . . 475

Chapter 35: Customizing the Examiner Interface . . . 476
About Customizing the Examiner User Interface . . . 476
The Tab Layout Menu . . . 477
Moving View Panels . . . 478
Creating Custom Tabs . . . 480
Managing Columns . . . 481
Customizing File List Columns . . . 481
Creating User-Defined Custom Columns for the File List view . . . 482
Deleting Custom Columns . . . 484
Navigating the Available Column Groups . . . 484

Chapter 36: Working with Evidence Reports . . . 486
Creating a Case Report . . . 487
Adding Case Information to a Report . . . 488
Adding Bookmarks to a Report . . . 489
Bookmark Export Options . . . 490
Adding Graphics Thumbnails and Files to a Report . . . 491
Adding a Video to a Report . . . 492
Adding a File Path List to a Report . . . 493
Adding a File Properties List to a Report . . . 494
Adding Registry Selections to a Report . . . 495
Adding Screen Captures from Examiner . . . 496
Selecting the Report Output Options . . . 497
Creating a Load File . . . 498
Customizing the Report Graphic . . . 500
Using Cascading Style Sheets . . . 501
Viewing and Distributing a Report . . . 501
Modifying a Report . . . 502
Exporting and Importing Report Settings . . . 502

Writing a Report to CD or DVD . . . 503

Part 6: Reference . . . 510

Chapter 37: Installing the AccessData Elasticsearch Windows Service . . . 511
About the Elasticsearch Service . . . 511
Prerequisites . . . 511
Installing the Elasticsearch Service . . . 512
Installing the Service . . . 512
Troubleshooting the AccessData Elasticsearch Windows Service . . . 513

Chapter 38: Installing the Windows Agent . . . 514
Supported Hashing Algorithms . . . 514
Manually Installing the Windows Agent . . . 514
Specific Instructions for eDiscovery . . . 514
Specific Instructions for AD Enterprise . . . 515
Installing the Agent . . . 516
Configuring Execname and Servicename Values . . . 518
Using Your Own Certificates . . . 520
Controlling Consumption of the CPU . . . 521
Important Information . . . 521

Chapter 39: Installing the Unix / Linux Agent . . . 522
Installing The Enterprise Agent on Unix/Linux . . . 522
Supported Platforms . . . 522
Uninstallation . . . 523
Configuration . . . 523
Starting the Service . . . 523
Stopping the Service . . . 524

Chapter 40: Installing the Mac Agent . . . 525
Configuring the AccessData Agent installer . . . 525
Bundling a Certificate . . . 525
Configuring the Port . . . 525
Additional Configuration Options . . . 526
Installing the Agent . . . 527
Uninstalling the Agent . . . 527

Chapter 41: Working with Windows Registry Evidence . . . 528
Understanding the Windows Registry . . . 528
Windows 9x Registry Files . . . 529
Windows NT and Windows 2000 Registry Files . . . 529
Windows XP Registry Files . . . 530

Possible Data Types . . . 531
Additional Considerations . . . 531
Windows XP Registry Quick Find Chart . . . 533
System Information . . . 533
Networking . . . 534
User Data . . . 534
User Application Data . . . 536

Chapter 42: Supported File Systems and Drive Image Formats . . . 537
File Systems . . . 537
Whole Disk Encrypted Products . . . 538
Hard Disk Image Formats . . . 538
CD and DVD Image Formats . . . 539

Chapter 43: Recovering Deleted Material . . . 540
FAT 12, 16, and 32 . . . 540
NTFS . . . 541
Ext2 . . . 541
Ext3 . . . 541
HFS . . . 541

Chapter 44: Managing Security Devices and Licenses . . . 542
Installing and Managing Security Devices . . . 542
Installing LicenseManager . . . 544
Starting LicenseManager . . . 545
Using LicenseManager . . . 546
Updating Products . . . 551
Sending a Dongle Packet File to Support . . . 552
Virtual CodeMeter Activation Guide . . . 553
Introduction . . . 553
Preparation . . . 553
Setup for Online Systems . . . 553
Setting up VCM for Offline Systems . . . 554
Creating a Virtual CM-Stick with Server 2003/2008 Enterprise Editions . . . 554
Additional Instructions for AD Lab WebUI and eDiscovery . . . 555
Virtual CodeMeter FAQs . . . 556
Network License Server (NLS) Setup Guide . . . 558
Introduction . . . 558
Preparation Notes . . . 558
Setup Overview . . . 558
Network Dongle Notes . . . 559
NLS Server System Notes . . . 559
NLS Client System Notes . . . 559

Chapter 45: Configuring a Multi-box Setup 561
Configuration for a Multi-box Setup 561
Configuration Overview. 561
Create a Service Account 561
Share the Case Folder 562
Configure Database Services 563
Share the Backup Destination Folder 563
Test the New Configuration 563

Chapter 46: AccessData Distributed Processing 565
Distributed Processing Prerequisites 565
Using PostgreSQL with Distributed Processing 566
Installing Distributed Processing 567
Configuring Distributed Processing 569
Using Distributed Processing 571
Checking the Installation 571

Chapter 47: AccessData Oradjuster 572
Oradjuster System Requirements 572
Introduction 572
The First Invocation 573
Subsequent Invocations 573
One-Box Deployment 573
Two-Box Deployment 574
Tuning for Large Memory Systems 576

Part 1

Introducing Forensic Toolkit® (FTK®)

This part contains introductory information about AccessData® Forensic Toolkit® (FTK®)and contains the following chapters:

- Introducing AccessData® Forensic Toolkit® (FTK®) (page 25)
- Getting Started with the User Interface (page 31)

Chapter 1

Introducing AccessData® Forensic Toolkit® (FTK®)

AccessData® Forensic Toolkit® (FTK®) lets you do thorough computer forensic examinations. It includes powerful file filtering and search functionality, and access to remote systems on your network.

AccessData forensic investigation software tools help law enforcement officials, corporate security, and IT professionals access and evaluate the evidentiary value of files, folders, and computers.

This chapter includes the following topics

- Overview of Investigating Digital Evidence (page 25)
- About Acquiring Digital Evidence (page 26)
- About Examining Digital Evidence (page 27)
- About Managing Cases and Evidence (page 28)
- What You Can Do With the Examiner (page 29)

Overview of Investigating Digital Evidence

This section describes acquiring, preserving, analyzing, presenting, and managing digital evidence and cases.

Forensic digital investigations include the following process

- Acquisition

  Acquisition involves identifying relevant evidence, securing the evidence, and creating and storing a forensic image of it.

  About Acquiring Digital Evidence (page 26)
- Analysis

  Analysis involves creating a case and processing the evidence with tools to properly investigate the evidence.

  About Examining Digital Evidence (page 27)
- Presentation

  Presentation involves creating a case report that documents and synthesizes the investigation.

  About Presenting Evidence (page 30)
- Management

  Management involves maintenance tasks such as backing up, archiving, detaching, attaching, restoring, and deleting cases and evidence.

  About Managing Cases and Evidence (page 28)

About Acquiring Digital Evidence

The admissibility of digital evidence in a court of law, can be dependent on preserving the integrity of the source data when it is acquired.

When digital evidence is acquired, forensic examiners create clones of the digital evidence to prevent any possibility of the digital evidence being changed or modified in any way. This acquired duplication is called a forensic image. If there is question to the authenticity of the evidence, the image can be compared to the original source data to prove or to disprove its reliability.

To create a forensic image, the data must be acquired in such a way that ensures that no changes are made to the original data or to the cloned data. The acquired data must be an exact “bit-by-bit” duplication of the source data. You can use AccessData’s Imager tool to acquire exact duplicates of digital evidence.

Preserving the evidence is accomplished both in the method of acquisition and the storage of the acquired data. Creating an exact replica of the original source is critical in forensic investigations. Keeping that replica safe from any source of corruption or unauthorized access involves both physical and electronic security. Once a case is created and the evidence is added to it, the case becomes just as critical. Acquired 001, E01, S01, and AD1 images can be encrypted using AD Encryption.

Types of Digital Evidence

Digital evidence is data such as documents and emails that can be transmitted and stored on electronic media, such as computer hard drives, mobile phones, and USB devices.

The following are types of digital evidence

- Static evidence

  The data that is imaged before it is added to a case is known as static evidence because it stays the same. Images can be stored and remain available to the case at all times because the image is an exact replica of evidence data in a file format.
- Live evidence

  Live evidence can be data that is acquired from a machine while it is running. It is often saved to an image as it is acquired. Sometimes, this is necessary in a field acquisition. Other times, it can be an original drive or other electronic data source that is attached to the investigation computer. All connections to the evidence should be made through a hardware write-blocking device. Live evidence that is attached to the investigation computer must remain connected throughout the entire investigation. It is best to create an image of any evidence source outside of your network, rather than risk having the source removed during the course of the investigation.
- Remote evidence

  Another type of live evidence is data acquired directly from machines that are connected to your corporate network. This live evidence is referred to as remote evidence. The process of adding it to your case for investigation is known as Remote Data Acquisition.

Acquiring Evidence

Some aspects of acquiring evidence are dependent on local or federal law. Be aware of those requirements before you acquire the evidence. You can utilize static evidence as well as acquire and use live and remote evidence from computers on your network.

About Acquiring Static Evidence

For digital evidence to be valid, it must be preserved in its original form. The evidence image must be forensically sound, in other words, identical in every way to the original. The data cannot be modified by the acquisition method used.

The following tools can do such an acquisition

- Hardware Acquisition Tools

  Duplicate, or clone, disk drives and allow read-only access to the hard drive. They do not necessarily use a CPU, are self-contained, and are often hand-held.

- Software Acquisition Tools

  Create a software duplication of the evidence called a disk image. Imager lets you choose the image file format, the compression level, and the size of the data segments to use.

Imager is a software acquisition tool. It can quickly preview evidence. If the evidence warrants further investigation, you can create a forensically sound disk image of the evidence drive or source. It makes a bit-by-bit duplicate of the media, rendering a forensic disk image identical in every way to the original, including file slack and allocated or free space.

You should use a write-blocking device when using software acquisition tools. Some operating systems, such as Windows, make changes to the drive data as it reads the data to be imaged.

You can process static evidence, and acquire live data from local network machines for processing. You can also view and preview evidence on remote drives, including CDs and DVDs.

About Acquiring Live Evidence

You can collect evidence from a live machine when you must. For criminal investigations, it is especially important to be aware of the data compromises you will face in such a situation, however sometimes there is no other choice. One such example is when the suspect drive is encrypted and you must acquire the image in-place while the machine is running. Another example is when imaging a RAID array; it must be live to be properly acquired.

About Acquiring Remote Evidence

You can acquire live evidence from your active networked computers, including information in RAM, and drive data. In addition, using Remote Drive Management System (RDMS), you can mount any drive through a mapping and browse its contents, then make a custom image of what you find. This type of evidence is known as remote evidence because it is not stored on the examiner computer but is within your network.

About Examining Digital Evidence

Analyzing evidence is a process to locate and identify meaningful data to make it available to the appropriate parties in an easy-to-understand medium.

After you have completed installation and created a case, you can add evidence for analysis. Evidence can include images of hard drives, floppy drives, CDs and DVDs, portable media such as USB drives, and/or live (un-imaged) data from any common electronic source.

The data can be hashed and indexed. You can run searches in the index for specific words like names and email addresses, or you can run live searches.

You can use the Known File Filter (KFF) library to categorize specific information during evidence analysis. The KFF lets you automatically assign files a status of Alert, Ignore, or Disregard.

About Managing Cases and Evidence

As you work with cases, it is a best practice to back up the cases and the evidence. Back up of evidence files is as easy as copying them to a secure location on a secure media. Back up of cases can be more complicated, but is equally important in the event of a crash or other catastrophic data loss.

Back up of a case requires the same amount of drive space as the case itself. This is an important consideration when planning your network resources for investigations.

Some of the case management features include: Archive, Archive and Detach, and Attach. These features give you control over your cases.

See Managing Global Features (page 48).

What You Can Do With the Examiner

You can use tab views to locate data such as the following

- The *Overview* tab lets you narrow your search to look through specific document types, or to look for items by status or file extension.
- The *Graphics* tab lets you quickly scan through thumbnails of the graphics in the case.
- The *Email* tab lets you view emails and attachments.

As you find items of interest, you can do the following

- Create, assign, and view labels in a sorted file list view.
- Use searches and filters to find relevant evidence.
- Create bookmarks to easily group the items by topic or keyword, find those items again, and make the bookmarked items easy to add to reports.
- Export files as necessary for password cracking or decryption, then add the decrypted files back as evidence.
- Add external, supplemental files to bookmarks that are not otherwise part of the case.

About Indexing and Hashing

During case creation and evidence import, you have the option to create an index of the data and to create hash numbers of all the files contained in the data.

Indexing is the process of creating an index with a searchable list of the words or strings of characters in a case. The index instantaneously provides results. However, it is sometimes necessary to use a live search to find things not contained in the index.

Hashing a file or files refers to the process of using an algorithm to generate a unique value based on a file's contents. Hash values are used to verify file integrity and identify duplicate and known files. Known files can be standard system files that can be ignored in the investigation or they can be files known to contain illicit or dangerous materials. Ignore and alert statuses provide the investigator with valuable information at a glance.

Three hash functions are available: Message Digest 5 (MD5), Secure Hash Algorithms 1 (SHA-1), and Secure Hash Algorithms 256 (SHA-256).

Typically, individual file hashes (each file is hashed as it is indexed and added to a case) compare the results with a known database of hashes, such as the KFF. However, you can also hash multiple files or a disk image to verify that the working copy is identical to the original.

About the Known File Filter Database

The Known File Filter (KFF) is an AccessData utility used to compare file hashes in a case against a database of hashes from files known to be ignorable (such as known system and program files) or with alert status (such as known contraband or illicit material), or those designated as disregard status (such as when a search warrant does not allow inspection of certain files within the image that have been previously identified). The KFF allows quick elimination or pinpointing of these files during an investigation.

Files which contain other files, such as ZIP, CAB, and email files with attachments are called container files. When KFF identifies a container file as either ignorable or alert, the component files are not extracted. If extraction is desired, the files must be manually extracted and added to the case.

See Using the Known File Filter (KFF) on page 264.

About Searching

You can conduct live searches or index searches of acquired images.

A live search is a bit-by-bit comparison of the entire evidence set with the search term and takes slightly more time than an Index search. Live searches allow you to search non-alphanumeric characters and to perform pattern searches, such as regular expressions and hex values.

See Searching Evidence with Live Search (page 376)

The Index search compares search terms to an index file containing discrete words or number strings found in both the allocated and unallocated space in the case evidence. The investigator can choose to generate an index file during preprocessing.

See Searching Evidence with Index Search (page 387)

AccessData products use dtSearch, one of the leading search tools available, in the index search engine. dtSearch can quickly search gigabytes of text.

About Bookmarking

As important data is identified from the evidence in the case, bookmarking that data enables you to quickly find and refer to it, add to it, and attach related files, even files that are not processed into the case. These files are called “supplementary files.” Bookmarks can be included in reports at any stage of the investigation and analysis.

See Bookmarking Evidence (page 364)

About Presenting Evidence

You can present digital evidence by creating a case report containing the evidence and investigation results in a readable, accessible format.

Use the report wizard to create and modify reports. A report can include bookmarks (information selected during the examination), customized graphic references, and selected file listings. Selected files, such as bookmarked files and graphics, can be exported to make them available with the report. The report can be generated in several file formats, including HTML and PDF and can be generated in multiple formats simultaneously.

See Working with Evidence Reports (page 486).

Chapter 2
Getting Started with the User Interface

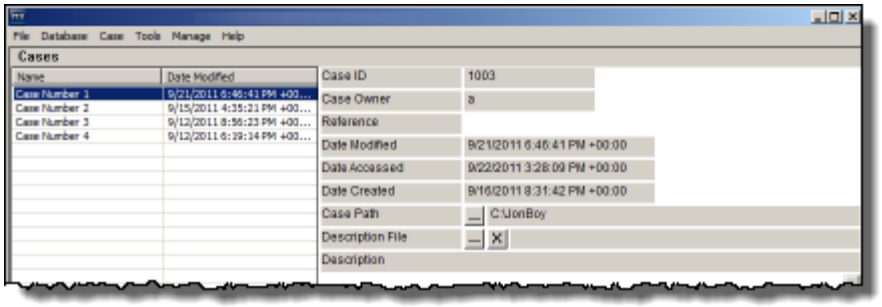
You can use two primary interfaces to work with cases and evidence:

- *Case Manager*
- *Examiner*

The Case Manager

You can use the *Case Manager* to manage application settings that apply to multiple cases.

The following is an example of the *Case Manager:*



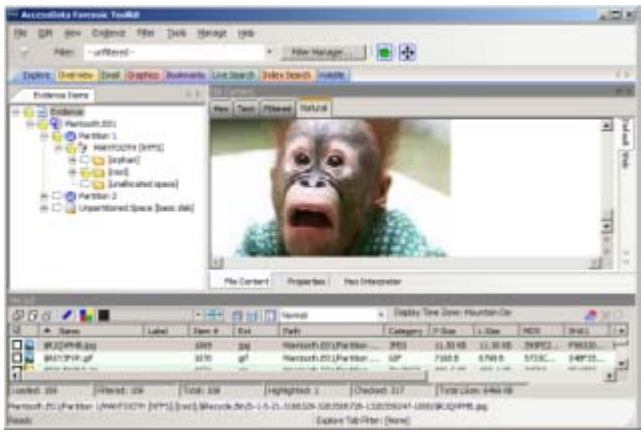
See Introducing Case Management on page 53.

The Examiner

You can use the *Examiner* to locate and interpret case data.

The following is an example of the *Examiner:*

The Examiner



For more information, see the following

- See Introducing Case Management (page 53)
- See Using the Examiner Interface (page 287)

Part 2

Administrating Forensic Toolkit® (FTK®)

This part contains information about administrating and configuring Forensic Toolkit® (FTK®) and contains the following chapters:

- Application Administration (page 34)

Chapter 3
Application Administration

This chapter includes topics that discuss administration tasks that you can do within the *Case Manager* interface.

See the following

- See Initializing the Database and Creating an Application Administrator Account on page 35.
- See Changing Your Password on page 36.
- See Recovering a Password on page 36.
- See Setting Database Preferences on page 38.
- See Managing Database Sessions on page 38.
- See Optimizing the Database for Large Cases on page 38.
- See Creating Databases for Individual Cases on page 39.
- See Managing KFF Settings on page 39.
- See Recovering and Deleting Processing Jobs on page 40.
- See Restoring an Image to a Disk on page 40.
- See Database Integration with other AccessData Products on page 41.
- See Adding New Users to a Database on page 42.
- See About Assigning Roles to Users on page 42.
- See Assigning Users Shared Label Visibility on page 47.
- See Setting Additional Preferences on page 47.
- See Managing Global Features on page 48.

Important: It is strongly recommended to configure antivirus to exclude the database (PostgreSQL, Oracle database, MS SQL) AD temp, source images/loose files, and case folders for performance and data integrity.

Initializing the Database and Creating an Application Administrator Account

The database and application must already be installed prior to this step.

The first time you launch the application, you specify the database to use. The application then creates the database schema which is required before any case data can be loaded into the database. You will be prompted to give the location of the database. This option allows a non-local database to be specified even if a local database is present.

After initializing the database, you are prompted to create an Application Administrator account. This account lets you create other user accounts and perform other administrative tasks.

To initialize the database and create an Application Administrator account

1. Click the shortcut icon to open the application
2. If it does not detect a configured database connection for this version, you will be prompted to *Add Database*.
3. In the *RDBMS* drop-down menu, select the brand of database that you are connecting to.
4. Specify the server hosting the database in the *Host* field.
   If the database is on the same computer as FTK, you can leave this field empty.
5. (Optional) Give the database connection a nickname in the *Display name* field.
6. Specify the database name by doing one of the following:
   - If you are using Oracle, you must configure the *Oracle SID* to be FTK2.
   - If you are using PostgreSQL or MS SQL Server, for the *PostgreSQL dbname* or *mssql sa,* you can use the default values or enter your own value. If you enter your own value, make sure that you record it so that you know the database name.
7. Do not change the *Port number* fields unless you have a custom database configuration.
8. If you are using MS SQL Server, you can check **Use Integrated Security** to use your Windows authentication credentials.
9. Click **OK.**
   If the connection attempt to the database was successful, the database will be initialized.
10. In the *Please Authenticate* dialog, log into the database using you database administrator account credentials.
    - If you used the default installation, enter the following credentials:
      Username: postgres
      Password: AD@Password
    - If you used the advanced installation or installed a different database, enter your credentials.

    A successful login initializes the database and opens the *Case Manager* window.
11. In the *Add New User* dialog, create an Application Administrator account for this version of the database schema.
    - Enter a name and password.
    - Record this information in a secure place.
12. Click **OK**.

Changing Your Password

Once logged into the system, you can change your password.

To change your password

1. In *Case Manager*, click **Database > Change Password**.
2. In the *Change Password* dialog box, enter your current password.
3. Enter your new password in the *New Password* text box.
4. Verify your new password by entering it again in the *Re-enter* text box.
5. Click **OK**.

Recovering a Password

You can recover an Administrator database password using a Password Reset File. Only the Administrator logged into the program can create the reset file and only the Administrator that created the reset file can use the file to reset the password. Before recovering your Administrator password, you will create a Password Reset File. Once you reset a password, the Password Reset File you used is no longer valid.

There are two main components to recover an Administrator's password:

- See Creating a Password Reset File on page 36.
- See Resetting your Password on page 37.

Creating a Password Reset File

You can use one of the following methods to create a Password Reset file:

- When creating a user with the Application Administration role and assigning a new password
- When changing the password for a user with the Application Administration role
- Accessing the Create Password Reset File option in the *Administer Users* dialog.

When creating/changing a password

1. After entering the new password, click **OK**.
2. A prompt appears that asks you to create a Password Reset File. Click **Yes**.
3. Navigate to a secure location and enter the name of the Password Reset File.

Important: Choose a location for the Password Reset File that only you know and to which others do not have immediate access. Keep its location confidential.

4. Click **OK**.

From the Administer Users dialog

1. In *Case Manager*, click **Database > Administer Users**.
2. Highlight your User Name (that is, the User Name under which you are logged in).
3. Click **Create Password Reset File**.
4. Navigate to a secure location and enter the name of the Password Reset File.

Important: Choose a location for the Password Reset File that only you know and to which others do not have immediate access. Keep its location confidential.

5. Click **OK**.

Resetting your Password

To reset your password, enter the Password Reset File you created previously.

Note: Any Password Reset Files that have already been used to reset passwords are no longer valid and will not work. Password Reset Files from other users or other databases also will not work. Only the Password Reset File that you created previously with your User Name and Password will work.

To enter the Password Reset File

1. When prompted for your password, enter your User Name.
2. Click **OK**.
   The **Reset Password** button appears in the *Please Authenticate* dialog.
3. Click **Reset Password**.
4. Locate the Password Reset File, highlight it, and click **OK**.
5. Enter a new password, verify the new password, and click **OK**.

Setting Database Preferences

The *Preferences* dialog lets you specify where to store the temporary file, the location of a network license and whether you want to optimize the database after you process evidence.

To set database preferences

1. In the *Case Manager*, click **Tools > Preferences**. Type in or browse to the folder you want temporary files to be written to.
2. Select a location for the temporary file folder.

   The Temporary File Folder stores temporary files, including files extracted from ZIP and email archives. The folder is also used as scratch space during text filtering and indexing. The Temporary File Folder is used frequently and should be on a drive with plenty of free space, and should not be subject to drive space allocation limits.
3. If your network uses AccessData Network License Service (NLS), you must provide the IP address and port for accessing the License Server.
4. Specify if you want to optimize the case database.

   This is set to optimize by default. Unmark the check box to turn off automatic optimization. This causes the option to be available in Additional Analysis for those cases that were processed with Optimize Database turned off initially. The Restore Optimization option in Additional Analysis does not appear if Database Optimization is set in the New Case Wizard to be performed following processing, or if it has been performed already on the current case from either place.
5. In the *Preferences* dialog, click **OK**.

Managing Database Sessions

You can use the *Sessions Management* dialog to manage and track database sessions from within the *Case Manager*. You can also use the *Manage DB Sessions* dialog to terminate cases that are open and consuming sessions, but are inactive. This lets open file handles close so that processing can be restarted.

To open the *Manage DB Sessions* dialog, in the *Case Manager*, click **Database > Session Management**.

Optimizing the Database for Large Cases

Note: This feature currently only supports installations using PostgreSQL. If you are using Oracle, this feature is disabled.

The database can be configured to optimize the handling of large cases. Specifically it may decrease the processing time for large cases. However, if you choose to optimize the database, it will require additional disk resources on the database host computer.

To optimize the database for large cases

1. In the *Case Manager*, click **Database > Configure**.
2. Click **Optimized for large cases**.
3. Click **Apply**.

Creating Databases for Individual Cases

Note: This feature only applies to MS SQL and PostgreSQL databases.

To improve performance, when you create new cases in FTK 6.0 or newer, a new database is created for each new case.

In addition to improved performance, if you configured the database location to be *in the case folder*, the database files are located under the case folder. This allows you to easily back up a case at the folder level as the case data and the database for the case are all under one case folder.

For example, if you create a case called *Investigation*, select the *In the case folder* option for the database location, and want to find the database files for that case, you could go to your *FTK Cases* folder (this is the file you listed as the case folder directory), click on the *Investigation* folder (this is the individual case folder), and open the *DB* folder, which contains all the database files for this case. If the *In the case folder* option is not selected, the database will be found in the appropriate Case folder located within the main MS SQL or PostgreSQL database files.

Important: Previous to FTK 6.0, all database files were stored within the main database and must be accessed through either the MS SQL or PostgreSQL database folder.

This feature is enabled by default.

To disable the individual case database feature

- In the *Case Manager*, click **Database > Put each case in its own DB**
  This will deselect the option and cases will be stored within the main database.

Managing KFF Settings

The AccessData Known File Filter can be managed from the *Case Manager* > *Manage* menu. Click **KFF** to open the *KFF Admin* dialog box.

This functionality is also found in the *Examiner* main window under *Manage* > *KFF.*

The functionality is the same regardless of how you launch KFF Admin.

See Using the Known File Filter (KFF) on page 281.

Recovering and Deleting Processing Jobs

Jobs that are started but unable to finish can be restarted or deleted.

To recover and delete processing jobs

1. Click **Tools > Recover Processing Jobs**. If no jobs remain unfinished, an error message pops up. Click **Continue** to see the *Recover Processing Jobs* dialog. It is be empty. Click **Close**. If there are jobs in the list, you can choose whether to *Restart* or *Delete* those jobs.
2. Click **Select All**, **Unselect All**, or mark the check box for each job to be recovered.
3. Do one of the following:
   - Click **Restart**. In the *Recovery Type* dialog, choose the recovery type that suits your needs.
   - Click **Delete**. Click **Yes** to confirm that you want to delete the job permanently.
4. Click **Close**.

Restoring an Image to a Disk

You can restore a disk image (001 (RAW/dd), E01, or S01) to a physical disk. The target disk must be the same size or larger than the original, uncompressed disk.

To restore an image to a disk

1. In the *Case Manager* or in the *Examiner*, click **Tools > Restore Image to Disk**. The *Restore Image to Disk* dialog opens.
2. Browse to and select the source image (must be RAW-dd/001, E01, or S01).
3. Click the *Destination drive* drop-down to choose the drive to restore the image to.

   If you have connected an additional target drive and it does not appear in the list, click **Refresh** to update the list.
4. If the target (destination) drive is larger than the original, uncompressed data, and you don't want the image data to share the drive space with old data, mark the **Zero-fill remainder of destination drive** check box.
5. If you need the operating system to see the target drive by drive letter, mark the **Notify operating system to rescan partition table when complete** check box.
6. Click **Restore Image**.

Database Integration with other AccessData Products

You can useFTK® 5.0 or higher with the following products:

- eDiscovery applications 5.x or higher
- AccessData Summation 5.x or higher
- AccessData CIRT 2.2 or higher

If you are using these products, you can share the same database. When you installFTK® , you can specify the same database that you are using for the other product. This lets you open and perform tasks on projects from those cases inFTK® . You can do the following tasks with projects:

- Open a case
- Backup and restore a case
- Add and remove evidence
- Perform Additional Analysis
- Search and index data
- Export data

Web Viewer

A single license of AccessData Summation is included with FTK 6.0 or higher. This tool allows you to conduct case assessment earlier with real-time collaboration. Attorneys or other teams have instant access to case data as it's being identified in FTK while incident responders are in the field or performing on-site collections.

For more information on how to use this feature, please reference the Summation product documentation found at summation.accessdata.com.

Multi-Case Search

Using the Summation Web Viewer, you can speed up the searching process by searching across multiple cases instead of one case at a time.

For more information on how to use this feature, please reference the Summation product documentation found at summation.accessdata.com.

Adding New Users to a Database

The Application Administrator can add new users to a database. The *Add New User* dialog lets you add users, disable users, change a user's password, set roles, and show disabled users.

To add a new user

1. Click **Database** > **Administer Users** > **Create User**.
2. In the *Add New User* dialog, enter information for the following:

User Name	Enter the name that the user is known as in program logs and other system information.
Full Name	Enter the full name of the user as it is to appear on case reports.
Password	Enter and verify a password for this user.
Role	Assign rights to the selected user name using roles. The default roles are: ● *Application Administrator*: Can perform all types of tasks, including adding and managing users. ● *Case/Project Administrator*: Can perform all of the tasks an Application Administrator can perform, with the exception of creating and managing users. ● *Case Reviewer*: Cannot create cases; can only process cases.

3. Click **OK** to apply the selected role to the new user.
4. Click **OK** to exit the *Add New User* dialog.

About Assigning Roles to Users

A user can have two levels of roles assigned to him or her. A user can have initial roles granted that apply globally across all cases in a database, and a user can also have specific roles granted for a specific case.

Roles can be granted as follows

- Roles that apply to all cases in a database are granted from the *Database* > *Administer Users* dialog.
- Roles that apply to a specific case are granted from the *Case* > *Assign Users* dialog.

The permissions that are applied through roles are cumulative, meaning that if you apply more than one, the greatest amount of rights and permissions become available.

When you assign roles that apply globally across the database, you cannot reduce the rights on a case-by-case basis.

AccessData recommends that when you first create a user account, save the account and close the dialog without setting a role. Then click **Case > Assign Users** to assign roles on a case-by-case basis. You can also assign all new users the Case Reviewer role for the database and, then selectively add additional roles as needed on a case-by-case basis.

There are pre-defined roles and you can create your own.

Tips for Assigning Permissions to Users

- It is important to understand that when you create user accounts (**Database > Administer Users**) and assign roles to users from that dialog, the roles you assign are global for this database; you cannot reduce their rights on a case-by-case basis.

- If you decide to limit a user's rights by assigning a different role, you must return to the **Database > Administer Users** dialog, select a user and choose **Set Roles**. Unmark the current role and click **OK** with no role assigned here, or choose a different role that limits access, then click **OK** to save the new setting.
- AccessData recommends that you first create the user account, save the account and close the dialog without setting a role. Then, click **Case > Assign Users** to assign roles on a case-by-case basis.
- Or you could assign all new users the global Case Reviewer role, then selectively add the Case/Project Administrator or Application Administrator role as needed. The permissions that are applied through roles are cumulative, meaning that if you apply more than one, the greatest amount of rights and permissions become available.

About Additional Roles

You can use the *Case Manager* to assign specific roles to users on a case-by-case basis. You can do this by using the *Additional Roles* feature.

For example, you may have a user who has a general role of *Case Reviewer*. However, you may want to give that user additional rights to a specific case. You can assign that user an *Additional Role* for that specific case. You could assign them a *Project/Case Administrator* role to grant some management rights, or you could assign them the *Application Administrator* role to gran them all rights for the case.

It is important to note that the rights granted through an *Additional Role* only apply once the user has opened the case in the *Examiner*. It does not grant them rights to the case using the *Case* or *Management* menus in the *Case Manager*. For example, this user cannot backup the case. To grant them rights at the *Case Manager* level, you would need assign them the regular *Project/Case Administrator* role, not as an *Additional Role*.

About Predefined Roles

The following roles are predefined and can easily be used:

- Application Administrator - has all rights
- Project/Case Administrator - has most rights to manage assigned cases and to create and manage new cases. (This role can only manage cases that the user is assigned to or has created themselves.)
- Case Reviewer - has rights to view data in assigned cases.

You can manage the rights that any role has.

The following tables display the default rights that the roles have or don't have.

Restrictions to the Case Reviewer Role

The case reviewer role does not have all of the permissions as the application administrator and the database administrator.

Permissions Denied to Case Reviewer Users

Create, Add, or Delete cases	Use Imager
Administer Users	Use Registry Viewer
Data Carve	Use PRTK
Manually Data Carve	Use Find on Disk
Assign Users to Cases	Use the Disk Viewer
Add Evidence	View File Sectors

Permissions Denied to Case Reviewer Users (Continued)

Access Credant Decryption from the Tools Menu	Define, Edit, Delete, Copy, Export, or Import Filters
Decrypt Files from the Tools Menu	Export Files or Folders
Mark or View Items Flagged as “Ignorable” or “Privileged”	Access the Additional Analysis Menu
Manage the KFF	Backup or Restore Cases
Enter Session Management	Create Custom Data Views

Differences Between the Case Administrator and Application Administrator Roles in the Examiner

Default Case Administrator and Application Administrator Role Comparison (In the Examiner)

Examiner Menu	Feature	Project/Case Administrator	Application Administrator
File	Export	x	x
	Export to Image	x	x
	Export Word List	x	x
	Reports	x	x
	Timeline Report	x	x
	Job Summary Report	x	x
	Export Event Audit Log	x	x
Evidence	Add/Remove	x	x
	Add Remote Data	x	x
	Additional Analysis	x	x
	Process Manually Carved Items		x
	Manage Evidence Group	x	x
	Import Memory Dump	x	x
	Import Custom Column File		x
	Import Custom Column Data		x
	Delete Custom Column Data		x
	Merge Case Index	x	x
Filter	New	x	x
	On	x	x
	Import	x	x

Default Case Administrator and Application Administrator Role Comparison (In the Examiner)

Examiner Menu	Feature	Project/Case Administrator	Application Administrator
	Tab Filter	x	x
Tools	Decrypt Files	x	x
	Verify Image Integrity		x
	Restore Image to Drive		x
	Mount Image to Drive	x	x
	Disk Viewer	x	x
	Other Applications > Imager, PRTK, Registry Viewer	x	x
	Custom Data Views		x
	Configure Agent Push	x	x
	Push Agents	x	x
	Manage Remote Acquisition	x	x
	Unmount Agent Drive	x	x
	Disconnect Agents	x	x
	Recover Processing Jobs	x	x
	Execute SQL		x
	Select Audit Events	x	x
Manage	KFF	x	x
	PhotoDNA	x	x
	Labels > Manage Shared Labels		x
	Carvers > Manage Carvers	x	x
	Carvers > Manage Shared Carvers		x
	Filters > Manage Filters	x	x
	Filters > Manage Shared Filters		x
	Columns > Manage Columns	x	x
	Columns > Manage Shared Columns		x

Assigning Initial Database-level Roles to Users

You can use the case manager to assign roles to users. Although the default roles can all be selected concurrently, AccessData recommends that only one of these be selected for any user to avoid granting either redundant or excessive permissions.

To assign initial database-level roles to users

1. In the *Case Manager*, click **Database > Administer Users**.
2. Do one of the following:
   - If the user does not yet exist in the system click **Create User** to create the user.
   - If the user does exist in the system, select the user's name and click **Set Roles**.
3. Click **Set Roles** to assign a role that limits or increases database and administrative access.
4. To assign a default role, mark the check box next to that role. The default roles are as follows:
   - *Application Administrator*: Can perform all types of tasks, including adding and managing users.
   - *Case/Project Administrator*: Can perform all of the tasks an Application Administrator can perform, with the exception of creating and managing users.
   - *Case Reviewer*: Cannot create cases; can only process cases.
5. Click **OK** to apply the selected role to the new user, save the settings, and return to the *Add New User* dialog.

Assigning Additional Case-level Roles to Users

You can use the *Case Manager* to assign specific roles to users on a case-by-case basis. You can do this by using the *Additional Roles* feature.

To assign additional case-level roles to users

1. In the *Case Manager*, select the case for which you want to grant additional roles to a user.
2. Click **Case > Assign Users**.
3. In the *Assigned Users* pane, select the user that you want to grant additional roles to.
4. Click **Additional Roles**.
5. In the *Additional Roles* dialog, under *Additional Roles for this Case*, select the roles that you want to grant.
6. Click **OK**.
7. Click **Done**.

Assigning Users Shared Label Visibility

Shared Labels give Application Administrators the added benefit of assigning visibility to only specific users on a case-by-case basis.

To assign Label Visibility

1. In *Case Manager*, click **Case > Assign Users**. The *Assign Users for Case* dialog opens, and a list of users that have permissions in the currently selected case appears.
2. Highlight a User.
3. Click **Label Visibility** to open the *Manage Label Visibility* dialog.

To show or hide Labels

1. Select a user in the *User List* pane. The *Shared Labels* dialog opens. Initially all are set as *Visible*.
2. Move labels as needed, based on the following:
   - Select a label you want that user not to see in any case, and click the **>** button.
   - To move a hidden label into the *Visible Labels* pane, select it, and click the **<** button.

Setting Additional Preferences

Choosing a Temporary File Path

The Temporary File Folder stores temporary files, including files extracted from ZIP and email archives. The folder is also used as scratch space during text filtering and indexing. The Temporary File Folder is used frequently and should be on a drive with plenty of free space, and should not be subject to drive space allocation limits.

To specify a location for the Temporary File Folder

1. In the *Case Manager*, click **Tools > Preferences**. Type in or browse to the folder you want temporary files to be written to.
2. Select the folder, then click **OK**.
3. In the *Preferences* dialog, verify the path is what you wanted.
4. In the *Theme to use for Visualization* section, you can also choose a color scheme to apply to the visualization windows.
5. Click **OK**.

Providing a Network Security Device Location

If your network uses AccessData Network License Service (NLS), provide the IP address and port for accessing the License Server.

Setting Theme Preferences for the Visualization Add on

To change the appearance of the Visualization window

1. In the *Case Manager*, click **Tools > Preferences**.
2. In the *Theme to use for Visualization* section, select a color scheme to apply to the Visualization windows.
3. Click **OK**.

Optimizing the Case Database

This is set to optimize by default. Unmark the check box to turn off automatic optimization. This causes the option to be available in Additional Analysis for those cases that were processed with Optimize Database turned off initially.

Note: The Restore Optimization option in Additional Analysis will not appear if Database Optimization was set in the New Case Wizard to be performed following processing, or if it has been performed already on the current case from either place.

Managing Global Features

Several features that were previously available only in a case are now fully implemented for global application, and are known as “Shared.” Since they are available globally, they are managed from the *Case Manager* interface, under the *Tools* menu.

The Application Administrators manage all Shared features. It is a good practice to set these up to the extent you are able, before you create your first case. Of course, new ones can be added at any time and copied to existing cases. Shared features can be created within cases by both Application and Case Administrators, and Shared (added to the global list).

Since each Shared feature has been documented to some extent in other chapters of the User Guide, only the parts of the features that apply specifically to Application Administrators are explained here. Cross-references are added to provide quick access to more complete information.

Managing Shared Custom Carvers

Carvers provide a comprehensive tool that allows you to customize the carving process to access hidden data exactly the way you need it. You can create new, and edit or delete existing shared carvers. In addition, you can import and export carvers, and copy carvers to cases that were previously processed without a particular custom carver.

There are no default carvers listed in the *Manage Shared Custom Carvers* dialog. It contains only custom-designed carvers that are shared.

See also Data Carving (page 108)

To create a Shared Custom Carver

1. In the *Case Manager*, click **Manage > Carvers.**
2. From the *Manage Shared Custom Carvers* dialog, click **New**.
3. Set the data carving options that you want to use.
4. Click **Save** when the new carver has been defined to meet your needs. You will see the new carver in this list and when you mark the **Carving** option in the *New Case Wizard*.
5. In the *Manage Shared Carvers* dialog, click the appropriate button to:
   - Create **New** shared custom carvers
   - **Edit** existing shared custom carvers
   - **Delete** shared custom carvers
   - **Import** shared custom carvers that have been exported from cases
   - **Export** shared custom carvers
   - **Copy** shared custom carvers to a case
6. Click **OK** to close the *Carving Options* dialog.

Managing Custom Identifiers

Custom File Identifiers let you specify which file category or extension should be assigned to files with a certain signature. While Custom Identifiers can be created and/or selected by a Case Administrator in the *New Case Wizard*, Shared Custom Identifiers are created and managed from a separate menu.

See also Creating Custom File Identifiers (page 115).

To Create a Shared Custom Identifier

1. In the *Case Manager*, click **Manage > Custom Identifiers**.
   Initially, the Custom Identifiers List pane is empty, and the rest of the window is grayed-out.
2. Click **Create New**. The window activates.
3. Enter a name for the new *Custom Identifier*. The name you enter is added into the *Custom Identifiers List*.
4. Enter a description to help define the identifier's purpose.
5. Create the *Custom Identifier* by defining *Operations* and using the *AND* and *OR* buttons.
6. When you are done defining this *Custom Identifier*, click **Apply**.

You can also do the following

- Click **Delete** to delete an unwanted or outdated identifier.
- Click **Export** to save the selected identifier as a `TXT` file.
- Click **Import** to add an external identifier file.
- Click **Close** to close the *Custom Identifiers* dialog.

Managing Columns

Shared Columns use the same windows and dialogs that Local Columns use.

To create a Shared Column Template

1. In *Case Manager*, click **Manage > Columns**.
   The *Manage Shared Column Settings* dialog opens.
2. Highlight a default *Column Template* to use as a basis for a *Custom Column Template*.
3. Click **New**.
4. Enter a new name in the *Column Template Name* field.
5. Select the Columns to add from the *Available Columns* pane, and click **Add >> t**o move them to the *Selected Columns* pane.
6. Select from the *Selected Columns* pane and click **Remove** to clear an unwanted column from the *Selected Columns*.
7. When you have the new column template defined, click **OK**.

See also Customizing File List Columns (page 480).

Managing File Extension Maps

Extension Maps can be used to define or change the category associated to any file with a certain file extension. For example, files with BAG extension which would normally be categorized as “Unknown Type” can be categorized as an AOL Bag File, or a files with a MOV extension that would normally be categorized as Apple QuickTime video files can be changed to show up under a more appropriate category since they can sometimes contain still images.

To create a Shared Custom Extension Mapping

1. In the *Case Manager*, click **Manage > File Extension Maps**.
2. In the *Custom Extension Mapping* dialog, click **Create New**.
3. Enter a name for the new mapping.
4. Enter a description for easier identification.
5. In the *Category* pane, select a file type you want to map an extension to.
6. Click **Add Extension**.
   The *Add New Extension* dialog box opens.
7. Enter the new extension to add.
8. Click **OK**.

You can also do the following:

- Click **Delete** to remove an unwanted or outdated mapping.
- Click **Import** to add an external Custom Extension Mapping file for Shared use.
- Click **Export** to save a Custom Extension Mapping file.
- Click **Close** to close the *Custom Extension Mapping* dialog.

See also Custom Case Extension Maps (page 116).

Managing Filters

Filters consist of a name, a description, and as many rules as you need. A filter rule consists of a property, an operator, and one or two criteria. (You may have two criteria in a date range.)

To create a new Shared filter

1. From *Case Manager*, click **Manage** > **Filters.**
   The *Manage Shared Filters* dialog opens.
2. Do one of the following:
   - If there is an existing filter in the *Filters* list that you want to use as a pattern, or template, highlight that filter and click **Copy**.
   - If there is no filter that will work as a pattern, Click **New**.
3. Enter a name and a short description of the new filter.
4. Select a property from the drop-down menu.
5. Select an operator from the **Properties** drop-down menu.
6. Select the applicable criteria from the **Properties** drop-down menu.
7. Each property has its own set of operators, and each operator has its own set of criteria. The possible combinations are vast.
8. Select the **Match Any** operator to filter out data that satisfies any one of the filter rules or the **Match All** operator to filter out data that satisfies all rules of the filter.
   You can test the filter without having to save it first. Check the **Live Preview** box to test the filter as you create it.

Part 3

Case Management

This part contains information about managing cases. It contains the following chapters:

- Introducing Case Management (page 53)
- Creating and Configuring New Cases (page 73)
- Managing Case Data (page 108)
- Working with Evidence Image Files (page 117)
- Working with Static Evidence (page 123)
- Working with Live Evidence (page 144)
- Filtering Data to Locate Evidence (page 158)
- Working with Labels (page 177)
- Decrypting Files (page 181)
- Exporting Data from the Examiner (page 202)
- Getting Started with KFF (Known File Filter) (page 257)
- Using the Known File Filter (KFF) (page 241)
- About Cerberus Malware Analysis (page 212)
- Running Cerberus Malware Analysis (page 230)

Chapter 4

Introducing Case Management

This chapter includes the following topics

- About Case Management (page 53)
- The User Interfaces (page 53)
- About the Cases List (page 54)
- Menus of the Case Manager (page 55)
- Menus of the Examiner (page 61)

About Case Management

Case management includes creating new cases, as well as backing up, archiving, detaching, restoring, attaching, deleting cases from the database, and managing case and evidence files.

Case management tasks are performed from the *Case Manager*.

Note: Multiple user names in a case are automatically assigned to Original User Names when a case is Archived, or Archived and Detached, and then restored. They can also be reassigned if necessary.

See Creating a Case (page 74)

See Managing Case Data (page 108)

The User Interfaces

The *Case Manager* lets you add and manage cases, users, roles and permissions, and do other management tasks. You can use the *Case Manager* to apply settings globally to all cases in the system.

Menus of the Case Manager (page 55)

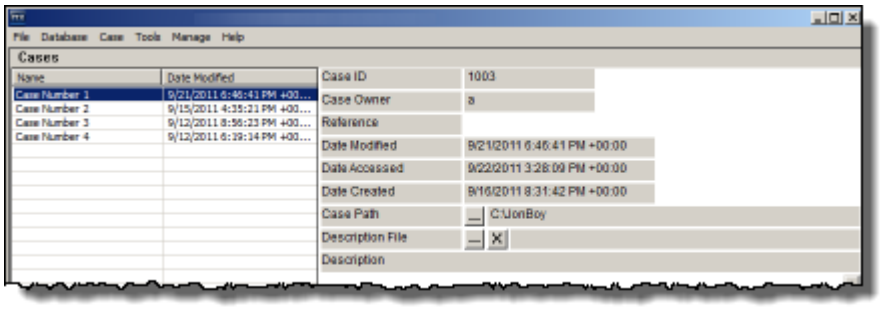
You can use the *Examiner* to locate, bookmark, and report on evidence.

Menus of the Examiner (page 61)

About the Cases List

The *Cases List* shows all of the cases that are available to the currently logged in user. The right pane displays information about the cases. The information that is shown for *Case File*, *Description File*, and *Description* are determined by the either the Application Administrator or the Case Administrator.

Case Manager Cases List



Menus of the Case Manager

Case Manager **Menus**

Menu	More Information
File	The *File* menu lets you exit the *Case Manager*. See Options of the Case Manager File Menu (page 55)
Database	The *Database* menu lets you administer users and roles. See Options of the Case Manager Database Menu (page 55)
Case	The *Case* menu lets you create, backup, and delete cases. You can also assign users to roles. *See* Options of the Case Manager Case Menu *(page 56)*
Tools	The *Tools* menu lets you configure the processing engine, recover interrupted jobs and restore images to a disk. See Options of the Case Manager Tools Menu (page 57)
Manage	The *Manage* menu lets you administrate shared objects such as columns, labels and carvers. See Options of the Case Manager Manage Menu (page 59)
Help	The *Help* menu lets you access the user guide as well as view version and copyright information. See Options of the Case Manager Help Menu (page 60)

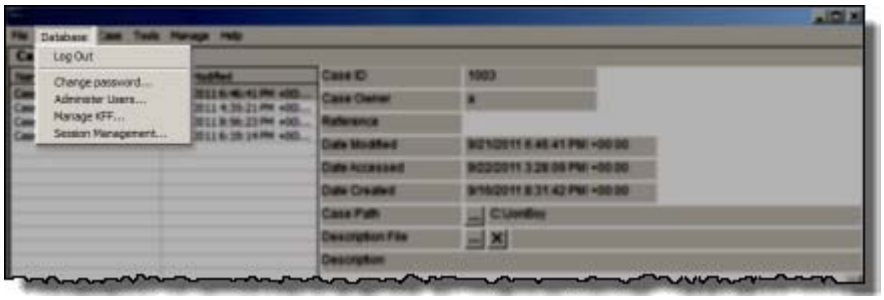
Options of the Case Manager File Menu

Options of the *Case Manager File* **Menu**

Option	Description
Exit	Exits and closes the program.

Options of the Case Manager Database Menu

Case Manager Database Menu

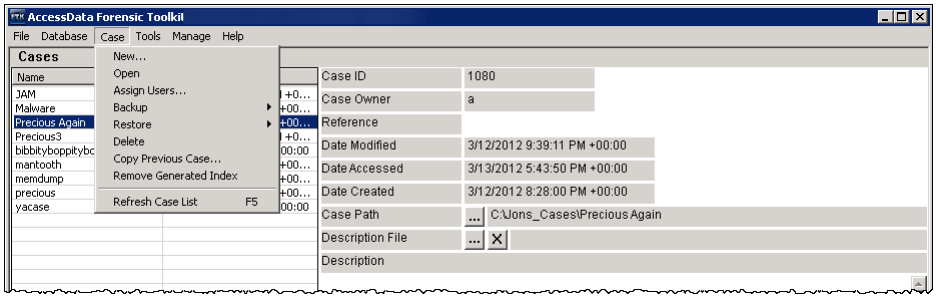


Options of the *Case Manager Database* Menu

Option	Description
Log In/ Log Out	Opens the authentication dialog for users to log into the database. You can log out the currently authenticated user without closing the program.
Put each case in its own DB	Creates a new database for each new case. This is enabled by default.
Change password	Opens the *Change Password* dialog. The currently authenticated user can change their own password by providing the current password, then typing and re-typing the new password. See Changing Your Password on page 36.
Administer Users	Lets you manage user accounts. The Application Administrator can change users' roles. See Adding New Users to a Database on page 42.
Session Management	Opens the *Manage Database Sessions* dialog. Click **Refresh** to update the view of current sessions. Click **Terminate** to end sessions that are no longer active. See Managing Database Sessions on page 38.
Configure	Opens the Configure Database dialog. See Optimizing the Database for Large Cases on page 38.

Options of the Case Manager Case Menu

Case Manager Case Menu

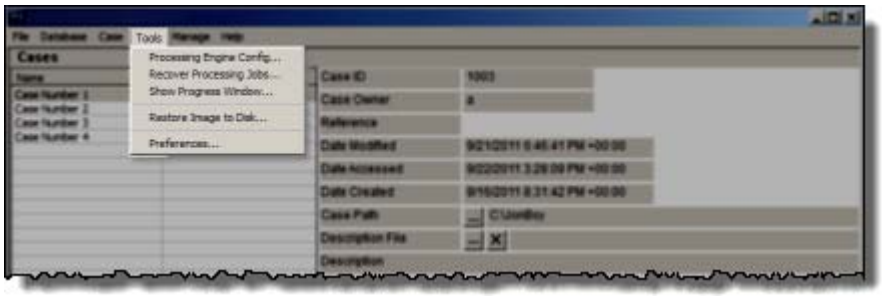


Options of the *Case Manager Case* Menu

Option	Description
New	Start a new case with the currently authenticated user as the Case Administrator. Case Reviewers cannot create a new case. See Creating a Case (page 74)
Open	Opens the highlighted case with its included evidence.
Assign Users	Allows the Application Administrator or the Case Administrator to adjust or control the rights of other users to access a particular case. Also allows the Administrator to control which users can see which of the Shared Labels that are available. See What You Can Do With Labels (page 177)
Backup	Opens a dialog for specifying names and locations for backup of selected cases. You can select multiple cases in the *Case Manager* to backup. Options are: ● Backup ● Archive ● Archive and Detach See Managing Case Data on page 108.
Restore	Opens a Windows Explorer instance for locating and restoring a selected, saved case. Options are: ● Restore an archived case ● Attach an archived and detached case See Managing Case Data on page 108.
Delete	Deletes the selected case. Pop-up appears to confirm deletion. See Deleting a Case on page 115.
Copy Previous Case	Copy a case from a previous version (4.2 or later) into the database. The use of a UNC folder path is no longer required beginning with version 4.2 and newer. To use copy from previous case you don't backup the case in the previous version, you simply use the “Copy Previous Case” feature. If you want to use Backup, you can backup the case in a previous version, such as 4.2 then restore it to the new version. Copy Previous Case doesn’t recognize backed-up cases.
Remove Generated Index	This option lets you select a case and delete its index. If you remove a case’s index, you cannot use index searches until you create a new index. To create a new index, in the *Examiner*, click **Evidence > Additional Analysis**. Select **dtSearch® Text Index** and click **OK**.
Refresh Case List	Right-click in the Case List area and select **Refresh Case List,** or click **F5** to refresh the case list with any new information.

Options of the Case Manager Tools Menu

Case Manager Tools Menu

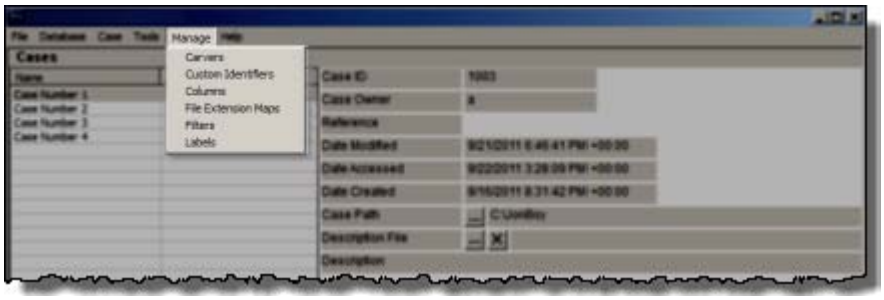


Options of the *Case Manager Tools* Menu

Option	Description
Processing Engine Config	Opens the *Processing Engine Configuration* dialog. Configure Remote Processing Engines here. Specify Computer Name/IP Address, and Port. Add New, Remove, Enable or Disable configured Processing Engines.
Recover Processing Jobs	Allows you to recover jobs that were interrupted during processing so the processing can be completed.
Show Progress Window	Opens the *Progress* window so you can check the Processing Status.
Restore Image to Disk	Copies a disk image to a disk other than the original.
Credant Server Settings	Lets you configure Credant server settings. See Decrypting Credant Files (Dell Data Protection | Encryption Server) on page 194.
Preferences	Opens *Preferences* dialog. See Setting Additional Preferences on page 47.

Options of the Case Manager Manage Menu

Case Manager Manage Menu

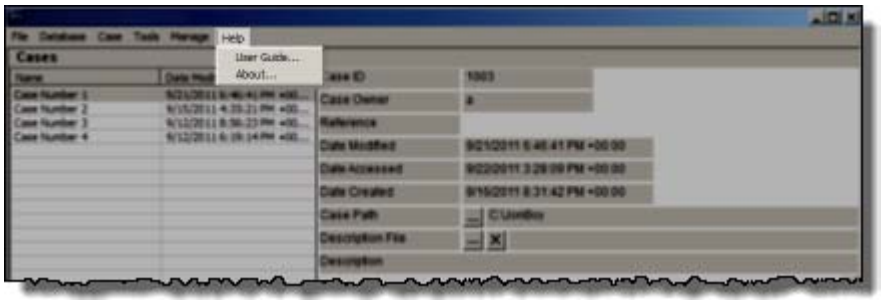


Options of the *Case Manager Manage* Menu

Option	Description
Carvers	Manage Shared Custom Carvers. Custom Carvers created here can be copied to cases. See Managing Shared Custom Carvers on page 48.
Custom Identifiers	Manage Shared Custom Identifiers. Custom Identifiers created here are automatically made available to all new cases, but cannot be copied directly to earlier cases. They must be exported and then imported into such cases. See Managing Custom Identifiers on page 49.
Columns	Manage Shared Column Settings. Custom Columns created here can be copied to cases. See Managing Columns on page 50.
File Extension Maps	Manage Shared File Extension Mappings. File Extension Maps created here are automatically made available to all new cases, but cannot be copied directly to earlier cases. They must be exported and then imported into such cases. See Managing File Extension Maps on page 50.
Filters	Manage Shared Filters. Custom Filters created here can be copied to cases. See Managing Filters on page 51.
Labels	Manage Shared Labels. Custom Labels created here can be copied to cases. See Working with Labels on page 177.
KFF	Lets you access advanced KFF management options such as creating groups and sets. See Getting Started with KFF (Known File Filter) on page 236.
PhotoDNA	Lets you configure a PhotoDNA Hash Library. See Using PhotoDNA to Compare Images on page 322.
Evidence Processing Profiles	Lets you configure Evidence Processing Profiles. See Using Processing Profiles on page 77.

Options of the Case Manager Help Menu

Case Manager Help Menu



Options of the *Case Manager Help* Menu

Option	Description
User Guide	Opens the user guide in PDF format.
About	Provides version and build information, copyright and trademark information, and other copyright and trade acknowledgements.

Menus of the Examiner

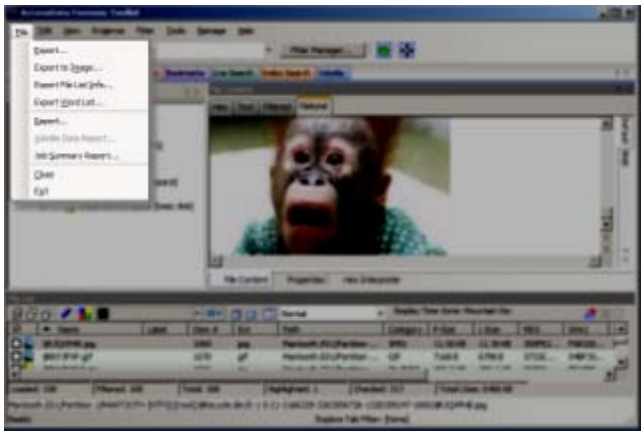
When a case is created and assigned a user, the *Examiner* window opens with the following menus:

Examiner Menus

Menu	Description
File	See Options of the Examiner File Menu (page 61)
Edit	See Options of the Examiner Edit Menu (page 62)
View	See Options of the Examiner View Menu (page 63)
Evidence	See Options of the Examiner Evidence Menu (page 65)
Filter	See Options of the Examiner Filter Menu (page 66)
Tools	See Options of the Examiner Tools Menu (page 67)
Manage	See Options of the Examiner Manage Menu (page 69)
Help	See Options of the Examiner Help Menu (page 71)

Options of the Examiner File Menu

Examiner File Menu



Options of the Examiner File Menu

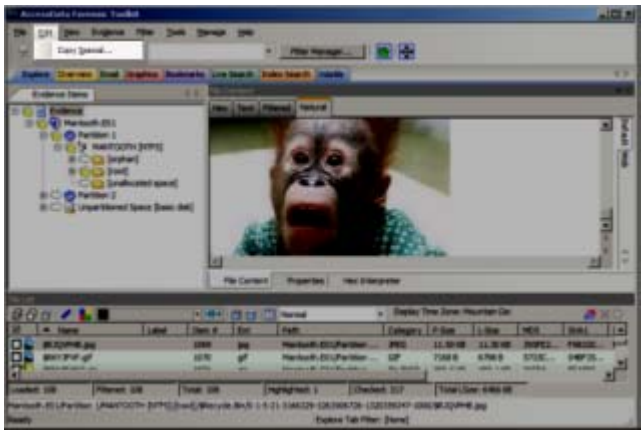
Option	Description
Export	Exports selected files and associated evidence to a designated folder.

Options of the Examiner File Menu (Continued)

Option	Description
Export to Image	Exports one or more files as an AD1 image to a storage destination. When exporting to AD1 the image's file path is added under a root directory. This speeds the process of gathering data for the AD1, and for shortening the path to AD1 content.
Export File List Info	Exports selected file information to files formatted as the Column List in CSV, TSV, and TXT formats.
Export Word List	Exports the words from the cases index as a text file. You can use this word list to create a dictionary in the AccessData PRTK and DNA products. See Exporting a Word List (page 211)
Export System Information	Exports system information when populated in the *System Information* tab. This option is grayed out unless System Information has been added to the case. See Viewing System Information on page 403.
Report	Opens the *Report Options* dialog for creating a case report. See Creating a Case Report (page 487)
Timeline Report	Opens the Timeline Report dialog for creating a Timeline bookmark report. See Creating a Timeline Bookmark Report on page 371.
Volatile Data Report	Opens a Volatile Data Report created from live data collected remotely and added to this case. This option is grayed out unless Volatile Data has been added to the case.
Job Summary Report	Opens an Evidence History report showing a job summary for all processing done within the case.
Close	Closes the *Examiner* and returns to the *Case Manager* window.
Exit	Closes both the *Examiner* and *Case Manager* windows.

Options of the Examiner Edit Menu

Examiner Edit Menu

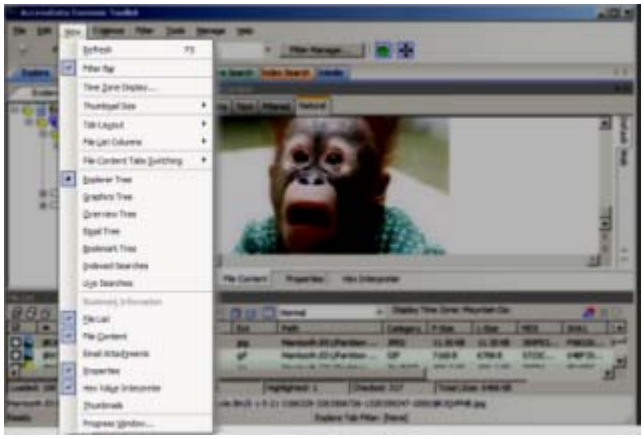


Options of the *Examiner Edit* Menu

Option	Description
Copy Special	Duplicates information about the object copied as well as the object itself, and places the copy in the clipboard. See Copying Information from the Examiner (page 202)

Options of the Examiner View Menu

Examiner View Menu



Options of the *Examiner View* Menu

Option	Description
Refresh	Reloads the current view with the latest information.

Options of the *Examiner View* Menu (Continued)

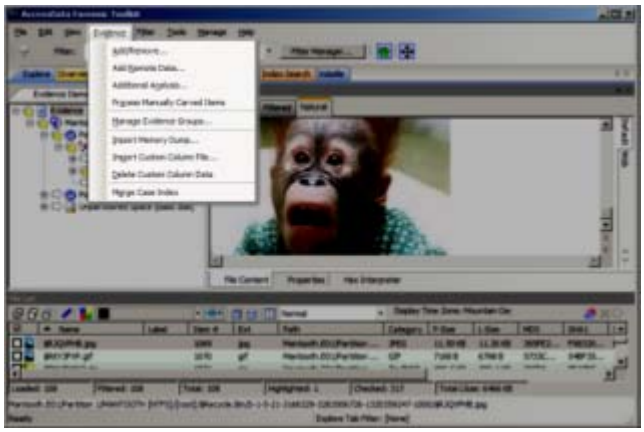
Option	Description
Filter Bar	Inserts the filter toolbar into the current tab. These features are also available from the Filter menu.
Time Zone Display	Opens the *Time Zone Display* dialog.
Thumbnail Size	Selects the size of the thumbnails displayed from the Graphics tab. Select from the following: ● Large-default ● Medium ● Small ● Tiny
Tab Layout	Manages tab settings. The user can lock an existing setting, add and remove settings, and save settings one tab at a time or all at once. The user can also restore previous settings or reset them to the default settings. These options are in the following list: ● Save ● Restore ● Reset to Default ● Remove ● Save All Tab Layouts ● Lock Panes ● Add New Tab Layout
FIle List Columns	Specifies how to treat the current File List. Options are: ● Save As Default ● Save All as Default ● Reset to Factory Default ● Reset All To Factory Default
File Content Tabs Switching	Specifies the behavior of file content when a different tab is selected. Options are: ● Auto ● Manual
Explore Tree	Displays the Explore Tree in the upper-left pane.
Graphics Tree	Displays the Graphics Tree in the upper-left pane.
Overview Tree	Displays the Overview Tree in the upper-left pane.
Email Tree	Displays the Email Tree in the upper-left pane.
Bookmark Tree	Displays the Bookmark Tree in the upper-left pane.
Index Searches	Displays the Index Search Results pane in the upper-left pane.
Live Searches	Displays the Live Search Results pane in the upper-left pane.
Bookmark Information	Adds the Bookmark Information pane into the current tab.
File List	Adds the File List pane into the current tab.

Options of the *Examiner View* Menu (Continued)

Option	Description
File Content	Adds the File Content pane into the current tab.
Email Attachments	Displays the attachments to email objects found in the case. Available only in the Email and Overview tabs.
Properties	Inserts the Object Properties pane into the current tab view.
Hex Value Interpreter	Displays a pane that provides an interpretation of Hex values selected from the Hex View pane.
Thumbnails	Displays a pane containing thumbnails of all graphics found in the case.
Video View	Displays a pane containing thumbnails of all videos found in the case.
Progress Window	Opens the *Progress* dialog, from which you can monitor tasks and/or cancel them.

Options of the Examiner Evidence Menu

Examiner Evidence Menu



Options of the *Examiner Evidence* Menu

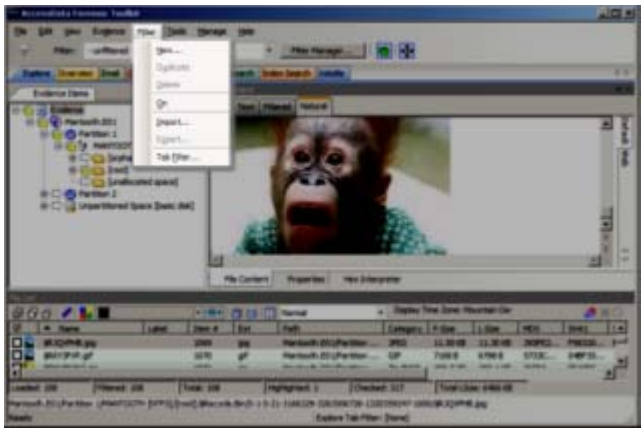
Option	Description
Add/Remove	Opens the *Manage Evidence* dialog, used to add and remove evidence. From Manage Evidence, choose from the following: Time Zone — Choose Time Zone for evidence item Refinement Options — Select Evidence Refinement Options Language Setting — Choose the language of the evidence item Define and Manage Evidence Groups Select Case KFF Options

Options of the *Examiner Evidence* Menu (Continued)

Option	Description
Add Remote Data	Opens the *Add Remote Data* dialog from which you can remotely access volatile, memory, and/or drive data and add it to the case. To Collect remote data from another computer on the network, provide the following: Remote IP Address Remote Port Select any or all of the following: Physical Drives (Can be mapped using RDMS) Logical Drives (Can be mapped using RDMS) Memory Analysis Click **OK** or **Cancel**.
Additional Analysis	Opens the *Additional Analysis* dialog with many of the same processing options available when the evidence was added. Allows the user to reprocess using available options not selected previously. See Using Additional Analysis (page 135).
Process Manually Carved Items	Initiates the processing of items that have been manually carved, using the selected options.
Manage Evidence Groups	Opens the dialog where you can create and manage Evidence Groups.
Import Memory Dump	Opens the *Import Memory Dump File* dialog which allows you to select memory dumps from other case files or remote data acquisitions, and import them into the current case. The memory dump file must have been previously created. See Working with Live Evidence (page 144)
Import Custom Column File	When a Custom Column Settings file has been created, import it into your case using this tool.
Delete Custom Column Data	If you have imported or created a Custom Column Settings file, use this tool to delete the associated column and its data from the view.
Merge Case Index	The processing engine does this automatically and no longer needs user interaction to select the merge.

Options of the Examiner Filter Menu

Examiner Filter Menu

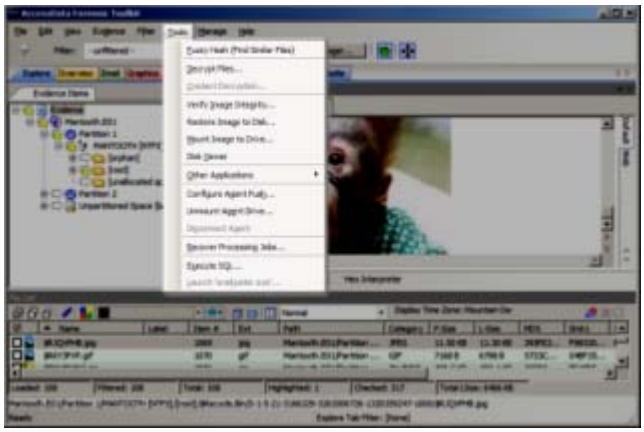


Options of the *Examiner Filter* Menu

Option	Description
New	Opens the *Filter Definition* dialog to define a temporary filter.
Duplicate	Duplicates a selected filter. A duplicated filter serves as a starting point for customizing a new filter.
Delete	Deletes a selected filter.
On	Applies the selected filter globally in the application. The File List changes color to indicate that the filter is applied.
Import	Opens the Windows file manager allowing the user to import a pre-existing filter.
Export	Opens the Windows File Manager allowing the user to save a filter. The name of the filter cannot have any special or invalid characters or the export will not work.
Tab Filter	Allows the selection of a filter to apply in the current tab.

Options of the Examiner Tools Menu

Examiner Tools Menu



Options of the *Examiner Tools* Menu

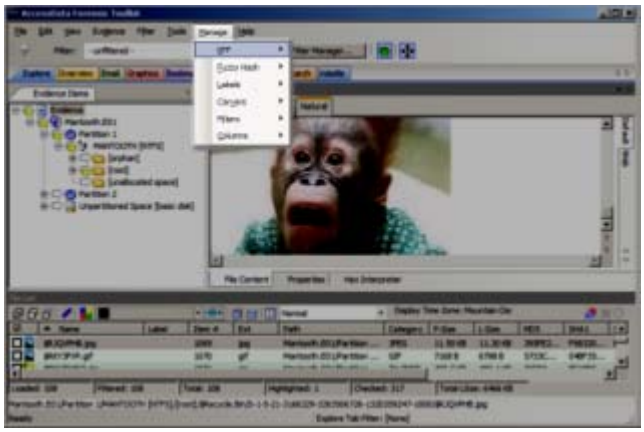
Option	Description
Decrypt Files	Decrypts EFS and Office files using passwords you enter. See Decrypting Files (page 181)
Credant Decryption	Opens the *Credant Decryption* dialog where you enter the decryption information. See Decrypting Credant Files (Dell Data Protection | Encryption Server) (page 194)
Send to DNA/PRTK for password recovery	Uses the integrated DNA/PRTK capabilities to decrypt several types of encrypted files. See Recovering Passwords using the PRTK/DNA Integrated Tool on page 188.
Verify Image Integrity	Generates hash values of the disk image file for comparison. See Verifying Drive Image Integrity (page 117)
Restore Image to Disk	Restores a physical image to a disk. If the original drive was on a bootable partition, the restored image may also be bootable. This feature is disabled for Case Reviewers.
Mount Image to Drive	Allows the mounting of a physical or logical image for read-only viewing. Logically mounting images allows them to be viewed as a drive-letter in Windows Explorer. Mounted logical drives now show the user the correct file, even when a deleted file with the same name exists in the same directory. See Mounting an Image to a Drive (page 118)
Disk Viewer	Opens a hex viewer that allows you to see and search contents of evidence items. Search Text for a term using Match Case, ANSI, Unicode, Regular Expression or Search Up instead of down; Search Hex using Search Up. Specify a logical sector or a cluster.
Other Applications	Opens other AccessData tools to complement the investigational analysis.

Options of the *Examiner Tools* Menu (Continued)

Option	Description
Configure Agent Push	Opens configuration dialog for pushing the agent to remote machines for data acquisition.
Push Agents	Push, or install, an Agent to a remote machine. You can Add, Remove, Import, or Export a single machine or a list of machines here.
Manage Remote Acquisition	Opens the *Remote Acquisition* dialog. Set the drive acquisition retry options here to set compression levels, balance speed of transfers with the amount of bandwidth usage, and set compression levels for remote data transfers.
Unmount Agent Drive	Unmount a remote drive that is mounted through RDMS.
Disconnect Agent	Disconnect a remote agent.
Recover Processing Jobs	Restarts processing so jobs that were interrupted can be completed.
Visualization	Lets you launch the Visualization add on module for the data that you currently have displayed in the File List Pane. Visualization is only available from the Explore, Overview, and Email Tabs. See Using Visualization on page 418.
Execute SQL	Executes a user-defined SQL script from within the interface.
Launch 'oradjuster.EXE'	Runs Oradjuster.EXE to temporarily optimize the available memory on the *Examiner* & database machine for those using an Oracle database. This utility does not work on a two-box configuration. See (page 572)

Options of the Examiner Manage Menu

Examiner Manager Menu



Options of the *Examiner Manage* Menu

Tool Type	Description
KFF	Manage Known File Filter (KFF) Library, sets, and groups. See Using the Known File Filter (KFF) (page 264).
PhotoDNA	Manage the PhotoDNA Hash Library See Using PhotoDNA to Compare Images (page 322)
Labels	Manage Local and Shared Labels as well as Label Groups. See What You Can Do With Labels (page 177).
Carvers	Manage Local and Shared Custom Carvers. See Data Carving (page 91).
Filters	Manage Local and Shared Filters. See Filtering Data to Locate Evidence (page 158).
Columns	Manage Local and Shared Columns. See Customizing File List Columns (page 481).

Options of the Examiner Help Menu

Options of the *Examiner Help* Menu

Option	Description
User Guide	Opens the user guide in PDF format.
Case Folder	Opens the folder that contains the case data.
About	Provides version and build information, copyright and trademark information, and other copyright and trade acknowledgements.

Chapter 5

Creating and Configuring New Cases

This chapter explains how to create a new case and configure the case options. If you have cases that were created in version 2.2 or later, you can convert them to the latest version.

This chapter includes the following topics

- Opening an Existing Case (page 73)
- Creating a Case (page 74)
- Configuring Detailed Options for a Case (page 75)
- Evidence Processing Options (page 82)
- Adding Evidence to a New Case (page 107)
- Converting a Case from Version 2.2 or Newer (page 107)

Opening an Existing Case

You can open a case that has previously been created and closed.

To open an existing case

1. Open the *Case Manager*.
2. In the *Case Manager*, highlight and double-click a case to open it.

Note: If you attempt to open a case you have not been assigned to, you will receive a message saying, “You have not been assigned to work on this case.” This is because you must be authenticated to open the case.

Creating a Case

Case information is stored in a database, and allows case administration as each new case is created.

To start a new case

1. Open the *Case Manager*.
2. Click **Case > New**. The *New Case Options* dialog opens.
3. Enter a name for the case in the *Case Name* field.
4. (Optional) Enter any specific reference information in the *Reference* field.
5. (Optional) Enter a short description of the case in the *Description* field.
6. You can use the *Description File* option to attach a file to the case. For example you can use this field to attach a work request document or a warrant to the case.
7. In the *Case Folder Directory* field specify where to store the case files. If you wish to specify a different location for the case, click the **Browse** button.

   Note: If the case folder directory is not shared, an error occurs during case creation.

8. (Optional) In the *Database Directory* field you can specify a location for where to store database directory files. You can check the *In the case folder* option to save the database directory in the case folder. If you do not specify these options, the database directory is saved to the default location of the database.

   Note: The location that you specify for *Database Directory* is relative to your database computer. If you intend to specify a location that is on a different computer than your database, for example in a multi-box scenario, then you must enter a network path.

Important: If using a UNC path for the case folder, and selecting the *In the case folder* option for the database directory, and if the database process isn't running as a network user, it will not be able to access the UNC path and will therefore fail to create the database files.

9. Configure the default processing options for the case by either using a processing profile or using custom settings.

   See Configuring Detailed Options for a Case on page 75.

10. If you wish to open the case as soon as it is created, mark **Open the case**.
11. Click **OK** to create the new case.

Configuring Detailed Options for a Case

When you configure Detailed Options for a case, there are options for doing the following:

- Configuring Default Processing Options for a Case (page 76)
- Configuring Evidence Refinement (Advanced) Options (page 100)
- Selecting Index Refinement (Advanced) Options (page 102)
- Managing Custom Identifiers (page 49)

About Processing Options

To help you in investigating the evidence in a case, the evidence data is processed. When evidence is processed, data about the evidence is created and stored in the database. You can view the processed data in the Examiner.

Evidence is processed at the following times:

- When adding evidence to a case
- After the initial processing, when performing an additional analysis

There are many different types of processing options. You can choose which processing options are relevant to your case.

The following are some examples of how your data can be processed:

- Generate hash values for all of the files in the evidence.
- Categorize the types of files in your evidence, such as graphics, office documents, encrypted files, and so on.
- Expand the contents of compound files, such as ZIP or TAR files.
- Create an index of the words that are in the evidence files for quick searches and retrieval.
- Create thumbnails for the graphics and videos in the evidence.
- Decrypt encrypted files.
- Compare files in your evidence against a list of known files that you may want to be alerted about (such as contraband images) or files that you want to ignore (such as Windows system files).

You can select processing options at the following times:

- When you create a case (Detailed Options) -- these become the default options for the case.
  See Evidence Processing Options (page 82)
- When you add evidence to an existing case (Refinement Options) -- you can either use or override the case defaults.
  See Configuring Evidence Refinement (Advanced) Options (page 100)
- When you perform an Additional Analysis on a case.
  See Using Additional Analysis (page 151)

Each processing option that you enable increases the time that it take to process the evidence. Depending on your situation, you may want to select more or fewer options.

For example, in one scenario, you may want to process the evidence as quickly as possible. In this case, you can use a pre-defined “Field Mode” that deselects almost all processing options and therefore takes the shortest

amount of time. After the initial processing, you can perform an Additional Analysis and enable additional processing options.

In another scenario, you may want to take the time to categorize and index files during the initial processing, so you can enable those options. This will take a significant amount of time for a large evidence set.

There is a Pause button available in the Data Processing Status window for situations where you need to interrupt evidence processing. Once you are ready to continue, select the Resume option.

Configuring Default Processing Options for a Case

When you create a case, you define the default processing options that are used whenever evidence is added to that case. By specifying default processing options for a case, you do not have to manually configure the processing options each time you add new evidence. The case-level defaults can be overridden and customized when you add new evidence or when you perform an additional analysis.

You configure the default processing options for a case in one of the following ways:

- Using Processing Profiles (page 77)
- Manually Customizing a set of Detailed Options (page 81)

Note: One factor that may influence which processing options to select is your schedule. If you disable indexing, it shortens case processing time. The case administrator can return at a later time and index the case if needed. The fastest way to create a case and add evidence is to use Field Mode.

Using Processing Profiles

About Processing Profiles

As an investigator, you may want to be able to save a set of processing options as a profile so that they can be easily reused. Processing profiles are a saved list of processing options that are stored in the database. Processing profiles are created at the global level and are available anytime you create a case.

For example, you may need to focus on certain types of data in a case, such as images and videos. In this example, you can create a processing profile that enables the following processing options:

- KFF
- Expand Compound Files
- Flag Bad Extensions
- Create Thumbnails for Graphics
- Create Thumbnails for Video
- Generate Common Video File
- Explicit Image Detection
- PhotoDNA

Each time you create this kind of case, you can use a profile with these options set as default and you won't need to manually specify them again.

Processing profiles are used at the case level. Specifically, when you create a case, you can select a processing profile from a drop-down list as the default processing options for that case. Any time that you add evidence to that case, the profile's setting will be the default "Refinement Options". This saves you time by not having to reconfigure processing options each time you add evidence to the case. However, when you add evidence to a case, you can modify the processing options for that evidence set. The profile is simply a set of default settings for the case.

Processing profiles are stored in the database. It is important to note that the profile itself does not get saved with the case but only the processing options that are in the profile.

There are five pre-defined, one-click processing profiles:

- Forensic processing (these were the Factory Defaults in version 4.x and earlier)
- eDiscovery processing
- Summation processing
- Basic assessment
- Field mode

See About Pre-configured Processing Profiles on page 78.

When you create a case, you can use one of the pre-configured profiles or create/select a custom profile. If you create a custom profile, you can save it with a unique name so that you can re-use it in a different case.

See Creating a Custom Processing Profile (page 79)

Important: When you create a custom profile, the settings for *Custom File Identification* or *Event Audit Log* options are not stored in the processing profile. The *Send Email Alert* and *Decrypt Credant Files* settings on the Evidence Processing tab are also not stored in the processing profile.

You can also edit, delete, import, or export custom processing profiles.

See Managing Processing Profiles (page 80)

You can also set custom processing options for a case without saving them to a profile.

See Manually Customizing a set of Detailed Options on page 81.

About Pre-configured Processing Profiles

There are five pre-defined, one-click processing profiles. You cannot edit, delete, or export these profiles. However, you can use them as a template for a new custom profile.

The following are the pre-configured profiles.

Forensic processing	This profile includes the following processing options: • MD5 Hash • SHA-1 Hash • SHA-256 Hash • Expand common compound files This will expand many types of compound files. See Expanding Compound Files (page 85) • File Signature Analysis • Flag Bad Extensions • dtSearch Test Index • Create Thumbnails for Graphics • Include Deleted Files • Include File Slack • Include Free Space • Include Message Headers • Create Email Threads This list of processing options is the same as the Factory Defaults in version 4.x. For a description of processing options, see Evidence Processing Options (page 82)
eDiscovery processing	The eDiscovery profile allows the processed evidence to be easily imported into AD eDiscovery. These options include: • MD5 Hash • Flag Duplicate Files • Expand Compound Files • File Signature Analysis • dtSearch Text Index • Document Content Analysis • Don’t Expand Embedded Graphics • Include Message Headers • Do not include document metadata in filtered text • Enable Advanced De-duplication Analysis • Propagate Email Attributes • Create Email Threads • Cluster Analysis • Include Extended Information in the Index

Summation processing	The Summation profile allows the processed evidence to be easily imported into AD Summation. These options include: ● Flag Duplicate Files ● Expand Compound Files ● File Signature Analysis ● Flag Bad Extensions ● dtSearch Text Index ● Create Thumbnails for Graphics ● Generate Common Video File ● Document Content Analysis ● Entity Extraction (Doc. Content) ● Don't Expand Embedded Graphics ● Include Message Headers ● Do not include document metadata in filetered text ● Enable Advanced De-duplication Analysis ● Propagate Email Attributes ● Create Email Threads ● Cluster Analysis ● Include Extended Information in the Index ● Enable 'Standard Viewer'
Basic assessment	This profile includes the following processing options: ● Expand Compound Files ● Include Deleted Files ● Include File Slack ● Include Free Space ● Include Message Headers
Field mode	FTK Field Mode disables the standard processing options when processing evidence. This speeds up processing. You can then re-enable processing options through Additional Analysis. See Using Additional Analysis (page 151) The Job Processing screen always shows 0 for Queued when Field Mode is enabled, because items move directly from Active Tasks to Completed.

Creating a Custom Processing Profile

You can create a processing profile by selecting a set of processing options and then saving them as a profile.

You can create a processing profile at one of the following times:

- Before creating a case
- While configuring processing options for a new case

To create a custom processing profile

1. From the Case Manager do one of the following:
   - To create a profile before creating a case, do the following:

   1a. Click **Manage > Evidence Processing Profiles**.

   1b. Click **New Profile**.
   You can use the Profile dropdown to select an existing profile as a template.

   - To create a profile while creating a new case, do the following:

1a. Click **Case > New**.

1b. In the *Processing profile* field, select one of the built-in options and click **Customize**.

2. Do the following:

2a. Click the *Evidence Processing* icon in the left pane, and select the processing options to be the default options for the case. For more information, see Evidence Processing Options (page 82).

2b. Click the *Evidence Refinement (Advanced)* icon to select the evidence refinement options to use on this case. For more information, see Configuring Evidence Refinement (Advanced) Options (page 100).

2c. Click the *Index Refinement (Advanced)* icon to select the index refinement options to use on this case. For more information, see Selecting Index Refinement (Advanced) Options (page 102).

2d. Click the *Evidence Lab/eDiscovery* icon to select the advanced options to use on this case. For more information, see Selecting Lab/eDiscovery Options (page 104).

Important: When you create a custom profile, the settings for *Custom File Identification* or *Event Audit Log* options are not stored in the processing profile. When you configure these options, the *Save As...* profile button is grayed out to signify that they are not saved as part of a profile.

See Managing Custom Identifiers (page 49).

3. When you are satisfied with your options, click **Save As...** or **Save user Profile...** to create the profile.

4. Enter a name for the profile.

- To create a new profile, enter a unique name.

  You cannot use *AD Standard, AD Field Mode*, or *Custom*.

- To update an existing custom profile, enter the profile name.

5. (Optional) Enter a description of the profile.

6. Click **Save**.

Managing Processing Profiles

You can do the following to manage processing profiles.

Edit	You can edit an existing custom profile. You cannot edit the five pre-configured profiles. To edit a profile, you select an existing profile, make the desired changes, save the profile, and confirm that you want to replace the existing profile.
Set as Default	You can set a processing profile as the global default. Whenever you create a new case, the default profile is listed. The default profile is denoted by a green check mark.
Delete	You can delete an existing custom profile. You cannot delete the five pre-configured profiles. If you delete a custom profile that has been selected as the default, the profile is deleted and the Forensic processing profile becomes the default.
Export	You can export a custom profile so that you can archive it or use it on a different computer. The exported settings are saved in xml format.
Import	You can import a profile that has been previously exported.

To manage processing profiles

1. In the Case Manager, click **Manage > Evidence Processing Profiles**.
2. In the *Manage Evidence Processing Profiles* dialog, select a profile to manage.
3. Select an action to perform on the profile.

4. Click **Close.**

Manually Customizing a set of Detailed Options

You can configure default processing options for a case without saving it as a profile.

To manually customize the evidence processing options

1. From the *New Case Options* dialog, click **Custom**.
   1a. Click the *Evidence Processing* icon in the left pane, and select the processing options to be the default options for the case. For more information, see Evidence Processing Options (page 82).
   1b. Click the *Evidence Refinement (Advanced)* icon to select the evidence refinement options to use on this case. For more information, see Configuring Evidence Refinement (Advanced) Options (page 100).
   1c. Click the *Index Refinement (Advanced)* icon to select the index refinement options to use on this case. For more information, see Selecting Index Refinement (Advanced) Options (page 102).
   1d. Click Custom File Identification to configure Custom Identifiers. For more information, see Managing Custom Identifiers (page 49).
2. Click **OK**.
   In the Processing Profile field, it will display *Custom* to show that you did not save the options as a profile.
3. When you are satisfied with your evidence refinement options, click **OK** to create the case and continue to the Evidence Processing screen.

Evidence Processing Options

The following table outlines the Evidence Processing options.

Evidence Processing Options

Process	Description
MD5 Hash	Creates a digital fingerprint using the Message Digest 5 algorithm, based on the contents of the file. This fingerprint can be used to verify file integrity and to identify duplicate files.
SHA-1 Hash	Creates a digital fingerprint using the Secure Hash Algorithm-1, based on the contents of the file. This fingerprint can be used to verify file integrity and to identify duplicate files.
SHA-256 Hash	Creates a digital fingerprint using the Secure Hash Algorithm-256, based on the contents of the file. This fingerprint can be used to verify file integrity and to identify duplicate files. SHA-256 is a hash function computed with 32-bit words, giving it a longer digest than SHA-1.
Flag Duplicate Files	Identifies files that are found more than once in the evidence. This is done by comparing file hashes.
KFF	Enables the Known File Filter (KFF) that lets you identify either known insignificant files that you can ignore or known illicit or dangerous files that you want to be alerted to. When you enable KFF, you must select a KFF Template to use. You can select an existing KFF Template from the drop-down menu or click **...** to create a new one. See Using the Known File Filter (KFF) on page 281.
PhotoDNA	Enables PhotoDNA which lets you compare images in your evidence against known images in a library. See Using PhotoDNA to Compare Images on page 331.
Expand Compound Files	Automatically opens and processes the contents of compound files such as ZIP, email, and OLE files. See Expanding Compound Files on page 85. The option *File Signature Analysis* is not forced to be selected. This lets you initially see the contents of compound files without necessarily having to process them. Processing can be done later, if it is deemed necessary or beneficial to the case by selecting *File Signature Analysis*.
Include Deleted Files	Checked by default. Un-check to exclude deleted files from the case.
File Signature Analysis	Analyzes files to indicate whether their headers or signatures match their extensions. This option must be selected if you choose Registry Summary Reports.
Flag Bad Extensions	Identifies files whose types do not match their extensions, based on the file header information. This option forces the *File Signature Analysis* option to be checked.

Evidence Processing Options (Continued)

Process	Description
Entropy Test	Identifies files that are compressed or encrypted. Compressed and encrypted files identified in the entropy test are not indexed.
dtSearch® Text Index	Stores the words from evidence in an index for quick retrieval. Additional space requirement is approximately 25% of the space required for all evidence in the case. Click **Indexing Options** for extensive options for indexing the contents of the case. Generated text that is the result of a formula in a document or spreadsheet is indexed, and can be filtered.
Create Thumbnails for Graphics	Creates thumbnails for all graphics in a case. Thumbnails are always created in JPG format, regardless of the original graphic file type. See Examining Graphics on page 324.
Create Thumbnails for Videos	Creates thumbnails for all videos in a case. You can also set the frequency for which video thumbnails are created, either by a percent (1 thumbnail every “n”% of the video) or by interval (1 thumbnail every “n” seconds. See Examining Videos on page 335.
Generate Common Video File	When you process the evidence in your case, you can choose to create a common video type for videos in your case. These common video types are not the actual video files from the evidence, but a copied conversion of the media that is generated and saved as an MP4 file that can be previewed on the video tab. See Examining Videos on page 335.
HTML File Listing	Creates an HTML version of the File Listing in the case folder.
CSV File Listing	The File Listing Database is now created in CSV format instead of an MDB file and can be added to Microsoft Access.
Data Carve	Carves data immediately after pre-processing. Click **Carving Options**, then select the file types to carve. Uses file signatures to identify deleted files contained in the evidence. All available file types are selected by default. For more information on Data Carving, see Data Carving (page 91).
Meta Carve	Carves deleted directory entries and other metadata. The deleted directory entries often lead to data and file fragments that can prove useful to the case, that could not be found otherwise.
Optical Character Recognition (OCR)	Scans graphics files for text and converts graphics-text into actual text. That text can then be indexed, searched and treated as any other text in the case. For more detailed information regarding OCR settings and options, see Running Optical Character Recognition (OCR) (page 95).

Evidence Processing Options (Continued)

Process	Description
Explicit Image Detection	Click **EID Options** to specify the EID threshold for suspected explicit material found in the case. See Evaluating Explicit Material on page 328. EID is an add-on feature. Contact your sales representative for more information.
Registry Reports	Creates Registry Summary Reports (RSR) from case content automatically. Click RSR Directory to specify the location of the RSR Templates. When creating a report, click the RSR option in the Report Wizard to include the RSR reports requested here. RSR requires that File Signature Analysis also be selected. If you try to select RSR first, an error will pop up to remind you to mark File Signature Analysis before selecting RSR.
Include Deleted Files	Enabled by default; to force exclusion of deleted files, unmark this check box.
Cerberus Analysis	Lets you run the add on module for Cerberus Malware Triage. You can click *Cerberus Options* to access additional options. For more information see About Cerberus Malware Analysis (page 229)
Send Email Alert on Job Completion	Opens a text box that allows you to specify an email address where job completion alerts will be sent. **Note:** Outgoing TCP traffic must be allowed on port 25. **Important:** These Emails are often filtered into Spam folders.
Decrypt Credant Files	See Decrypting Credant Files (Dell Data Protection | Encryption Server) on page 208. If you select to decrypt Credant files, the *File Signature Analysis* option will automatically be selected as well.
Process Internet Browser History for Visualization	Processes internet browser history files so that you can see them in the detailed visualization timeline. See Visualizing Browser History Data on page 294.
Perform Automatic Decryption	Disabled by default. Attempts to decrypt files using a list of passwords that you provide See About Decrypting Files on page 195.
Language Identification	Disabled by default. Analyzes the first two pages of every document to identify the languages contained within. The user will be able to filter by a Language field within review and determine who needs to review which documents based on the language contained within the document. See Identifying Document Languages on page 352.
Document Content Analysis	Disabled by default. Analyzes the content and groups it according to topic in the *Overview* tab. When selected, the DCA Options button is also activated and opens the Document Content Analysis Options. See Using Document Content Analysis on page 414.

Evidence Processing Options (Continued)

Process	Description
Entity Extraction (Document Content)	Disabled by default. Identifies and extracts specific types of data in your evidence. You can select to process one or all of the following types of entity data: • Credit Card Numbers • Phone Numbers • Social Security Numbers In the *Examiner*, under the *Document Content* node in the *Overview* tab, you can view the extracted data. See Using Entity Extraction on page 410.
Generate System Information	Extracts data and populates the *System Information* tab. See Viewing System Information on page 410.

If you expand data, you will have files that are generated when the data was processed and was not part of the original data. There are tools to help you identify generated data.

See Identifying Processing-Generated Data on page 342.

See Relating Generated Files to Original Files on page 342.

Expanding Compound Files

You can expand individual compound file types. This lets you see child files that are contained within a container such as ZIP files. You can access this feature from the *Case Manager*'s new case wizard, or from the *Add Evidence* or *Additional Analysis* dialogs.

See Evidence Processing Options on page 82.

Unless noted, the following file types are expanded by default.

If you expand data, you will have files that are generated when the data was processed and were not part of the original data. There are tools to help you identify generated data.

See Identifying Processing-Generated Data on page 342.

See Relating Generated Files to Original Files on page 342.

You can expand the following compound files:

7-ZIP	
Active Directory	
AOL Files	
Blackberry IPD backup file	
BZIP2	
Cellebrite UFDR	Not expanded by default. See Examining Mobile Phone Data on page 361.
Chrome Bookmarks	Not expanded by default. See About Expanding Google Chrome, Firefox, and IE 9 Data on page 356.

Chrome Cache	Not expanded by default. See About Expanding Google Chrome, Firefox, and IE 9 Data on page 356.
Chrome SQLite	Not expanded by default. See About Expanding Google Chrome, Firefox, and IE 9 Data on page 356.
DBX	
ESE DB	Expands ESE (Extensible Storage Engine) databases. See About Extensible Storage Engine (ESE) Databases on page 355.
EMFSPOOL	
EVTX	Not expanded by default. See Viewing Data in Windows XML Event Log (EVTX) Files on page 343.
EXIF	
Facebook Messenger (Android)	Not expanded by default. See Working with Facebook Messenger (Android) on page 369.
Firefox Cache	Not expanded by default. See About Expanding Google Chrome, Firefox, and IE 9 Data on page 356.
Firefox JSON	Not expanded by default. See About Expanding Google Chrome, Firefox, and IE 9 Data on page 356.
Firefox SQLite	Not expanded by default. See About Expanding Google Chrome, Firefox, and IE 9 Data on page 356.
GZIP	
IE Cookie Text	Not expanded by default. See About Expanding Data from Internet Explorer (IE) Version 10 or Later on page 357.
IE Recovery	Not expanded by default. Expands *IE Recovery* data that was stored when access to a Web site was lost. See Expanding Internet Artifact Data on page 359.
IE WebCache	Not expanded by default. Expands the Web cache data for IE 10 and later IE versions. See About Expanding Data from Internet Explorer (IE) Version 10 or Later on page 357.
IIS log files	Not expanded by default. See Viewing IIS Log File Data on page 345.
Internet Explorer Files	Expands Internet Explorer internet artifact data. See Expanding Internet Artifact Data on page 359.
iOS Backup	Not expanded by default. See Working with iOS Backup on page 368.
Log2t CSV	Not expanded by default. This processing option will recognize CSV files that are in the Log2timeline format and parses the data within the single CSV into individual records within the case. The individual records from the CSV will be interspersed with other data, giving you the ability to perform more advanced timeline analysis across a very broad set of data. In addition you can leverage the visualization engine to perform more advanced timeline based visual analysis. See Viewing Log2Timeline CSV File Data on page 349.
Lotus Notes (NSF)	
MBOX	
Mail.ru Chat	Parses Mail.RU Agent chat history files and email (mra.dbs). Examining Internet Artifact Data (page 354)
Microsoft Exchange	
MS Office, OLE and OPC documents	

MSG	
Outlook for Mac OLM	
PDF	
PKCS7 and S/MIME Files	
PST	
RAR	
Registry	Not expanded by default. See Viewing Registry Timeline Data on page 347.
RFC822 Internet Email	
Skype SQLite	Not expanded by default. See Expanding Internet Artifact Data on page 359.
SQLite Databases	
TAR	
Unistore Database (Windows 10 Mail)	Not expanded by default. See Processing Windows 10 Email and Contacts on page 324.
Windows Thumbnails	
XRY	
ZIP, including ZIPX	

Be aware of the following before you expand compound files:

- If you have labeled or hashed a family of files, then later choose to expand a compound file type that is contained within that label or family, the newly expanded files do not inherit the labeling from the parent, and the family hashes are not automatically regenerated.
- Many Lotus Notes emails, *.NSF, are being placed in the wrong folders in the *Examiner*.

  This is a known issue wherein Lotus Notes routinely deletes the collection indexes. Lotus Notes client has the ability to rebuild the collections from the formulas, but *Examiner* cannot. So if Lotus Notes data is acquired shortly after the collections have been cleared, then the *Examiner* does not know where to put the emails. These emails are all placed in a folder named "[other1]."

  To work around: Open the NSF file in the Lotus Notes client, and then close (you may need to save), then acquire the data and process it. The emails will all be in the right folder because the view collections are recreated.
- Compound file types such as AOL, Blackberry IPD Backup, EMFSpool, EXIF, MSG, PST, RAR, and ZIP can be selected individually for expansion. This feature is available from the *Case Manager* new case wizard, or from the *Add Evidence* or *Additional Analysis* dialogs.
- Only the file types selected are expanded. For example, if you select **ZIP**, and a **RAR** file is found within the **ZIP** file, the **RAR** is not expanded.

To expand compound files

1. Do one of the following:
   - For new cases, in the *New Case Options* dialog click **Detailed Options**.
   - For existing cases, in the *Examiner*, click **Evidence > Additional Analysis**.
2. Select **Expand Compound Files**.

   The option *File Signature Analysis* is no longer forced to be checked when you select **Expand Compound Files**. This lets you see the contents of compound files without necessarily having to process them. You can choose to process them later, if it is deemed necessary or beneficial to the case.
3. Select **Include Deleted Files** if you also want to expand deleted compound files.
4. Click **Expansion Options**.

5. In the *Compound File Expansions Options* dialog do the following:
   - If you do not want to expand office documents that do not have embedded items, select **Only expand office documents with embedded items**.
   - Select the types of compound files that you want expand.

     Only the file types that you select are expanded. For example, if you select ZIP, and a RAR file is contained within the ZIP file, then the RAR is not expanded.

   Note: The option *File Signature Analysis* is not forced to be selected. This lets you initially see the contents of compound files without necessarily having to process them. Processing can be done later, if it is deemed necessary or beneficial to the case by selecting *File Signature Analysis*.
6. In the *Compound File Expansions Options* dialog, click **OK**.
7. Click **OK**.

Using dtSearch Text Indexing

You can use the following indexing options to choose from when creating a new case.

Indexing a Case

All evidence should be indexed to aid in searches. Index evidence when it is added to the case by checking the dtSearch Text Index box on the *Evidence Processing Options* dialog, or index after the fact by clicking and specifying indexing options.

Scheduling is another factor in determining which process to select. Time restraints may not allow for all tasks to be performed initially. For example, if you disable indexing, it shortens the time needed to process a case. You can return at a later time and index the case if needed.

dtSearch Indexing Space Requirements

To estimate the space required for a dtSearch Text index, plan on approximately 25% of the space needed for each case's evidence.

Configuring Case Indexing Options

Case Indexing gives you almost complete control over what goes in your case index. These options can be applied globally from *Case Manager*.

Note: Search terms for pre-processing options support only ASCII characters.

These options must be set prior to case creation.

To set Indexing Options as the global default

1. In *Case Manager*, click **Case > New > Detailed Options.**
2. In the *Evidence Processing* window, mark the **dtSearch Text Index** check box.
3. Click **Indexing Options** to bring up the *Indexing Options* dialog box.
4. Set the options using the information in the following table:

dtSearch Indexing Options

Option	Description
Letters	Specifies the letters and numbers to index. Specifies Original, Lowercase, Uppercase, and Unaccented. Choose **Add** or **Remove** to customize the list. You may need to add characters to this list for specific index searches to function properly. For example, you may want to do an index search for 'name@domain.com'. By default, the @ symbol is treated as a space and is not indexed. See Spaces on page 90. To have the @ symbol included in the index, you would need to do two things: ● Remove the @ from the *Spaces* list. Add the @ to the *Letters* list.
Noise Words	A list of words to be considered "noise" and ignored during indexing. Choose **Add** or **Remove** to customize the list.
Hyphens	Specifies which characters are to be treated as hyphens. You can add standard keyboard characters, or control characters. You can remove items as well.
Hyphen Treatment	Specifies how hyphens are to be treated in the index. Options are: ● Ignore Hyphens will be treated as if they never existed. For example, the term "counter-culture" would be indexed as "counterculture." ● Hyphen Hyphens will be treated literally. For example, the term "counter-culture" would be indexed as "counter-culture." ● Space Hyphens will be replaced by a non-breaking space. For example the term "counter-culture" would be indexed as two separate entries in the index being "counter" and "culture." ● All Terms with hyphens will be indexed using all three hyphen treatments. For example the term "counter-culture" will be indexed as "counterculture", "counter-culture", and as two separate entries in the index being "counter" and "culture."

dtSearch Indexing Options (Continued)

Option	Description
Spaces	Specifies which special characters should be treated as spaces. Remove characters from this list to have them indexed as any other text. Choose **Add** or **Remove** to customize the list. You may need to remove characters from this list for specific index searches to function properly. For example, you may want to do an index search for 'name@domain.com'. By default, the @ symbol is treated as a space and is not indexed. To have the @ symbol included in the index, you would need to do two things: ● Remove the @ from the *Spaces* list. Add the @ to the *Letters* list.
Ignore	Specifies which control characters or other characters to ignore. Choose **Add** or **Remove** to customize the list.
Max Word Length	Allows you to set a maximum word length to be indexed.
Index Binary Files	Specify how binary files will be indexed. Options are: ● Index all ● Skip ● Index all (Unicode)
Enable Date Recognition	Choose to enable or disable this option.
Presumed Date Format For Ambiguous Dates	If date recognition is enabled, specify how ambiguous dates should be formatted when encountered during indexing. Options are: ● MM/DD/YY ● DD/MM/YY ● YY/MM/DD
Set Max Memory	Allows you to set a maximum size for the index.
Auto-Commit Interval (MB)	Allows you to specify an Auto-Commit Interval while indexing the case. When the index reaches the specified size, the indexed data is saved to the index. The size resets, and indexing continues until it reaches the maximum size, and saves again, and so forth.

Note: The *Indexing Options* dialog does not support some Turkish characters.

5. When finished setting Indexing Options, click **OK** to close the dialog.
6. Complete the *Detailed Options* dialog.
7. Click **OK** to close the *Detailed Options* dialog.
8. Specify the path and filename for the *Default Options* settings file.
9. Click **Save**.
10. In the *Case Manager*, click **Case > New**.
11. Proceed with case creation as usual. There is no need to click *Detailed Options* again in creating the case to select options, unless you wish to use different settings for this case.

In addition to performing searches within the case, you can also use the Index to export a word list to use as a source file for custom dictionaries to improve the likelihood and speed of password recovery related to case files

when using the Password Recovery Toolkit (PRTK). You can export the index by selecting *File* > *Export Word List*. See also Searching Evidence with Index Search (page 394)

Data Carving

Data carving is the process of looking for data on media that was deleted or lost from the file system. Often this is done by identifying file headers and/or footers, and then “carving out” the blocks between these two boundaries.

AccessData provides several specific pre-defined carvers that you can select when adding evidence to a case. In addition, Custom Carvers allow you to create specific carvers to meet your exact needs.

Data carving can be selected in the New Case Wizard as explained below, or from within the *Examiner*. In addition, because Custom Carvers are now a Shared feature, they can be accessed through the Manage menu. These are explained below.

Pre-defined Carvers

The following pre-defined carvers are available. Some carvers are enabled by default.

Pre-defined Carvers

Carver	Enabled by default?
AOL bag files	Yes
BMP files	Yes
EMF files	Yes
GIF files	Yes
HTML files	Yes
JPEG files	Yes
LNK files	Yes
OLE files (MS Office)	Yes
PDF files	Yes
PNG files	Yes
TIFF files	Yes
ZIP files	Yes
AIM Chat Logs	No
EML	No
Facebook Status Updates	No
Facebook Chat	No
Facebook Email Artifact	No
Facebook Mail Snippets	No
Facebook Fragment	No
Gmail Email Message	No
Gmail Parsed Email	No
Google Talk Chats	No

Pre-defined Carvers (Continued)	
Hotmail Email Artifact	No
Bebo Chat	No
Firefox Form History	No
Firefox Places	No
Firefox Session Store	No
Frostwire Props Files	No
GigaTribe Chat	No
IE8 Recovery URL	No
Limewire Props	No
Limewire/Frostwire Keyword Search	No
mIRC Chat Log	No
MySpace Chat	No
Twitter Status	No
Windows Messenger Plus w/chat logging	No
MSN/WLM Chat	No
Yahoo Diagnostic	No
Yahoo Webmail Chat	No
Yahoo Mail	No
Yahoo Group Chat Recvd	No
Yahoo Group Chat Sent	No
Yahoo Chat	No
Yahoo Chat UnAllocated	No
Yahoo Unencrypted Active	No

Selecting Data Carving Options

If you are unfamiliar, please review Creating a Case (page 74) and Configuring Detailed Options for a Case (page 75) before beginning this section.

When you are in the New Case Wizard in **Detailed Options > Evidence Processing**, click **Data Carve > Carving Options** to open the dialog shown below.

If you already have a case open with evidence added and processed, click the following:

- **Evidence > Additional Analysis > Data Carve > Carving Options**

Standard Data Carving gives you a limited choice of which file types to carve.

Choose which types of data to carve according to the information below.

To set Data Carving options

1. Select *Data Carve*.
2. Click *Carving Options*.

3. Select the types of files you want carved.
   - Click *Select All* to select all file types to be carved.
   - Click *Clear All* to unselect all file types.
   - Click on individual file types to toggle either selected or unselected.

   Note: It may help to be aware of the duplicate files and the number of times they appear in an evidence set to determine intent.

4. Depending on the file type highlighted, the Selected Carver Options may change. Define the optional limiting factors to be applied to each file:
   - Define the minimum byte file size for the selected type.
   - Define the minimum pixel height for graphic files.
   - Define the minimum pixel width for graphic files
5. Mark the box, **Exclude KFF Ignorable** files if needed.
6. If you want to define Custom Carvers, click **Custom Carvers**. (Custom Carvers are explained in the next section.) When you are done with Custom Carvers, click **Close**.
7. In the *Carving Options* dialog, click **OK**.

Custom Carvers

The *Custom Carvers* dialog allows you to create your own data carvers in addition to the built-in carvers. Custom Carvers can be created and shared from within a case, or from the *Case Manager*.

Application Administrators have the necessary permissions to access the *Manage Shared Carvers* dialog. Case Administrators can manage the Custom Carvers in the cases they administer. Case Reviewers are not allowed to manage Custom Carvers.

Shared Custom Carvers are automatically available globally; but can be copied to a case when needed. Carvers created within a case are automatically available to the case, but can be shared and thus made available globally.

To access *Manage Custom Carvers* dialogs, click **Manage > Carvers > Manage Custom Carvers** (or **Manage Shared Carvers** if you are an Application Administrator).

The *Manage Shared Custom Carvers* and *Manage Custom Carvers* dialogs are very similar. The difference is whether you can copy the carvers to a case or make the carvers shared.

The *Custom Carvers* dialog allows you to define carving options for specific file types or information beyond what is built-in. Once defined, these carving options files can be Shared with the database as well as exported and imported for use in other cases. The original, local copy, remains in the case where it was created, for local management.

To create a Custom Data Carver

1. Click **New**.
2. Complete the data fields for the Custom Carver you are creating. Options are as follows:

Name	Name of the Carver
Author	Name of the Creator
Description	Summarizes the intended use of the carver

Minimum File Size in bytes	(Optional)
Maximum File Size in bytes	(Optional) The default Custom Carver Maximum File Size is 2147483647 bytes. The carver Max File Size in bytes must be populated with any size larger than the defined Minimum File Size in bytes (default is 0). A Maximum File Size equal to or less than the minimum size, or <no entry>, results in an error prompting for a valid number to be entered.
File extension	Defining the extension of the carved file helps with categorization, sorting, and filtering carved files along with other files in the case.
Key Signature(s) and Other Signature(s)	Enter the ASCII text interpretation of the file signature as seen in a hex viewer. Many can be defined, but at least one key signature must be present in the file in order to be carved. Click the + icon to begin defining a new Key Signature or Other Signature. Click the - icon to remove a defined Key Signature or Other Signature.
File Category	The File Category the carved item will belong to once it is carved. The specified category must be a leaf node in the *Overview* tab.
Offset	Use decimal value.
Length	The length in bytes.
Little Endian	If not marked, indicates Big Endian.
Signature	Enter the ASCII text interpretation of the file signature as seen in a hex viewer.
Case Insensitive	Default is case sensitive. Mark to make the end File Tag Signature not case sensitive.

3. When done defining the Custom Carver, click **Close**.

Note: When adding signatures to a carver, the **Signature is case sensitive** check box is used when carving for signatures that can be both upper or lower case. For example, <HTML> and <html> are both acceptable headers for HTML files, but each of these would have a different signature in hex, so therefore they are case sensitive.

- The objects and files carved from default file types are automatically added to the case, and can be searched, bookmarked, and organized along with the existing files.

  However, custom carved data items are not added to the case until they are processed, and they may not sort properly in the File List view. They are added to the bottom of the list, or at the top for a Z-to-A search, regardless of the filename.

Running Optical Character Recognition (OCR)

The Optical Character Recognition (OCR) process lets you extract text that is contained in graphics files. The text is then indexed so that it can be, searched, and bookmarked.

Running OCR against a file type creates a new child file item. The graphic files are processed normally, and another file with the parsed text from the graphic is created. The new OCR file is named the same as the parent graphic, [graphicname.ext], but with the extension OCR, for example, graphicname.ext.ocr.

You can view the graphic files in the *File Content View* when it is selected in the *File List View*. The *Natural* tab shows the graphic in its original form. The *Filtered* tab shows the OCR text that was added to the index.

Before running OCR, be aware of the following:

- OCR is only a helpful tool for the investigator to locate images from index searches. OCR results should not be considered evidence without further review.
- OCR can have inconsistent results. OCR engines by nature have error rates. This means that it is possible to have results that differ between processing jobs on the same machine with the same piece of evidence.
- Some large images can cause OCR to take a very long time to complete. Under some circumstances, they may not generate any output.
- Graphical images that have no text or pictures with unaligned text can generate bad output.
- OCR is best on typewritten text that is cleanly scanned or similarly generated. All other picture files can generate unreliable output that can vary from run to run.

To run Optical Character Recognition

1. Do one of the following:
   - For new cases, in the *New Case Options* dialog click **Detailed Options**.
   - For existing cases, in the *Examiner*, click **Evidence > Additional Analysis**.
2. Select **Optical Character Recognition**. OCR requires *File Signature Analysis* and *dtSearch Indexing* to be selected. When *Optical Character Recognition* is marked, the other two options are automatically marked and grayed-out to prevent inadvertent mistakes, and ensure successful processing.
3. Click **OCR Options**.
4. In the *OCR Options* dialog, select from the following options:

Options	Description
File Types	Lets you specify which file types to include in the OCR process during case processing. For PDF files, you can also control the *maximum filtered text size* for which to run OCR against.
Filtering Options	Lets you specify a range in file size to include in the OCR process. You can also specify whether or not to only run OCR against black and white, and grayscale. The *Restrict File Size* option is selected by default. By default, OCR file generation is restricted to files larger than 5K. If you do not want to limit the size of OCR files, you must disable this option.
Engine	Lets you choose the OCR engine to use.

5. In the *OCR Options* dialog, click **OK**.

6. In the *Evidence Processing* dialog, click **OK**.

Optical Character Recognition (OCR) Confidence Score

There is an option to show the confidence score for each file that has been processed with OCR. It is recommended to use this feature to sort documents processed using OCR to determine which files may need to be manually reviewed for the desired keywords.

The OCR Confidence Score value may be one of the following:

Options	Description
1-100%	The OCR confidence % score for a document that had a successful OCR process; the higher the score, the higher the confidence.
No Score Available (2)	The OCR results are from a previous version.
Minimal Confidence (1)	The OCR extraction is not in a supported language or is not clear.
No Text Found (0)	The OCR process did not identify any text to extract.
OCR Skipped (-1)	The OCR process was skipped due to some condition.
OCR Extraction Error (-2)	The OCR process failed for that file.
Blank	The file does not need the OCR process; for example, a .DOC file or email.

Note: For data that is upgraded from a previous version, if a file has been previously processed with OCR, it will show a value of 2. You can use the *Additional Analysis* tool, found in the *Evidence* menu, to re-OCR the document and you will get the new OCR confidence score.

To use the OCR Confidence Score

1. Process your data using the *Optical Character Regocnition* option.
   See Running Optical Character Recognition (OCR) on page 95.
2. Add the *OCR Graphic* column to the *File List.*
   See Managing Columns on page 480.
3. Sort the *File List* using the *OCR Graphic* column
   Use the scores shown in the *File List* to determine which items should be reviewed for keywords.

Using Explicit Image Detection

About Explicit Image Detection

Explicit Image Detection (EID) is an add-on feature. Contact your sales representative for more information. EID reads all graphics in a case and assigns both the files and the folders they are contained within a score according to what it interprets as being possibly illicit content. The score ranges are explained later in this section.

To add EID evidence to a case

1. Click **Evidence > Add/Remove**.
2. In the **Detailed Options > Evidence Processing** dialog, ensure that **File Signature Analysis** is marked.
3. Select **Explicit Image Detection**
4. Click **EID Options**.The three EID options are profiles that indicate the type of filtering that each one does. You can choose between any combination of the following profiles depending on your needs:

Profile Name	Level	Description
X-DFT	Default (XS1)	This is the most generally accurate. It is always selected.
X-FST	Fast (XTB)	This is the fastest. It scores a folder by the number of files it contains that meet the criteria for a high likelihood of explicit material. It is built on a different technology than X-DFT and does not use “regular” DNAs. It is designed for very high volumes, or real-time page scoring. Its purpose is to quickly reduce, or filter, the volume of data to a meaningful set.
X-ZFN	Less False Negatives (XT2)	This is a profile similar to X-FST but with more features and with fewer false negatives than X-DFT. You can apply this filter after initial processing to all evidence, or to only the folders that score highly using the X-FST option. Check-mark or highlight those folders to isolate them for Additional Analysis. In Additional Analysis, File Signature Analysis must be selected for EID options to work correctly.

5. When the profile is selected, click **OK** to return to the *Evidence Processing* dialog and complete your selections.

AccessData recommends that you run *Fast (X-FST)* for folder scoring, and then follow with *Less False Negatives (X-ZFN)* on high-scoring folders to achieve the fastest, most accurate results.

After you select *EID* in *Evidence Processing* or *Additional Analysis*, and the processing is complete, you must select or modify a filter to include the EID related columns in the *File List View*.

Including Registry Reports

The Registry Viewer supports Registry Summary Report (RSR) generation as part of case processing.

To generate Registry Summary Reports and make them available for the case report

1. Ensure that **File Signature Analysis** is marked.
2. Mark **Registry Reports**.
3. Click **RSR Directory.**
4. Browse to the location where your RSR templates are stored.
5. Click **OK**.

Send Email Alert on Job Completion

You can select to send an email notification when a job completes.

This option is also available from **Evidence > Additional Analysis**. Enter the email address of the recipient in the *Job Completion Alert Address* box, then click **OK**.

Note: Outgoing TCP traffic must be allowed on port 25.

Custom File Identification Options

Custom File Identification provides the examiner a way to specify which file category or extension should be assigned to files with a certain signature. These dialogs are used to manage custom identifiers and extension maps specific to the case.

In *Detailed Options,* the *Custom File Identification* dialog lets you select the Custom Identifier file to apply to the new case. This file is stored on the system in a user-specified location. The location can be browsed to, by clicking **Browse**, or reset to the root drive folder by clicking **Reset**.

Creating Custom File Identifiers

Custom File Identifiers are used to assign categories to files that may or may not already be automatically categorized in a way that is appropriate for the case. For example, a file that is discovered, but not categorized, will be found under the “Unknown Types” category. You can prevent this categorization before the evidence is processed by selecting a different category and sub-category.

Custom Identifiers provide a way for you to create and manage identifiers, and categorize the resulting files into any part of the category tree on the Overview tab. You can select from an existing category, or create a new one to fit your needs.

You can define identifiers using header information expected at a specific offset inside a file, as is now the case, but in addition, you can categorize files based on extension.

Note: PDF files are now identified through the PDF file system and will no longer be identified through Custom File Identification.

To create a Custom Identifier file

1. In the *Case Manager*, click **Case > New > Detailed Options**.
2. Click **Custom File Identification**.
3. Below the *Custom Identifiers* pane on the left of the *Custom File Identification* dialog, click **New**. The *Custom Identifier* dialog opens.

4. Fill in the fields with the appropriate values. The following table describes the parameters for Custom File Identifiers:

Parameter	Description
Name	The value of this field defines the name of the sub-category that will appear below the selected Overview Tree category and the category column.
Description	Accompanies the Overview Container's tree branch name.
Category	The general file category to which all files with a matching file signature should be associated.
Offset	The decimal offset of where the unique signature (see Value) can be found within the file given that the beginning of the file is offset 0.
Value	Any unique signature of the file expressed in hexadecimal bytes.

Note: The Offset must be in decimal format. The Value must be in hexadecimal bytes. Otherwise, you will see the following error: Hex strings in the Offset field cause an exception error.

"Exception: string_to_int: conversion failed was thrown."

Important: After creating a Case Custom File Identifier, you must apply it, or it will not be saved.

5. When you are done defining the Custom File Identifier, click **Make Shared** to share it to the database. This action saves it so the Application Administrator can manage it.
6. Click **OK** to close the dialog. Select the identifier you just created and apply it to the case you are creating. Otherwise it will not be available locally in the future.

Custom Case Extension Maps

Extension Maps can be used to define or change the category associated to any file with a certain file extension. For example, files with BAG extension, which would normally be categorized as "Unknown Type," can be categorized as an AOL BAG file, or files with a MOV extension, that would normally be categorized as Apple QuickTime video files, can be changed to show up under a more appropriate category since they can sometimes contain still images.

To create a Case Custom Extension Mapping

1. Within the *Detailed Options* dialog of the *New Case* wizard, select **Custom File Identification** on the left hand side.
2. Under the *Extension Maps* column, click **New**.
3. Fill in the fields with the appropriate values.

4. Mark **Make Shared** to share this Custom Extension Mapping with the database.
   Shared features such as Custom Extension Mappings are managed by the Application Administrator. Your copy remains in the case for you to manage as needed.

   The following table describes the parameters for Custom Extension Mappings

Parameter	Description
Name	The value of this field defines the name of the sub-category that will appear below the selected Overview Tree category and the category column.
Category	The general file category to which all files with a matching file signature should be associated.
Description	Accompanies the Overview Container's tree branch name.
Extensions:	Any file extension that should be associated to the selected Category.

Note: You must use at least one offset:value pair (hence the [...]+), and use zero or more OR-ed offset:value pairs (the [...]*). All of the offset:value conditions in an OR-ed group are OR-ed together, then all of those groups are AND-ed together.

Configuring Evidence Refinement (Advanced) Options

The Evidence Refinement Options dialogs allow you to specify how the evidence is sorted and displayed. The Evidence Refinement (Advanced) option allows you to exclude specific data from being added to the case when found in an individual evidence item type.

Many factors can affect which processes to select. For example, if you have specific information otherwise available, you may not need to perform a full text index. Or, if it is known that compression or encryption are not used, an entropy test may not be needed.

Important: After data is excluded from an evidence item in a case, the same evidence cannot be added back into the case to include the previously excluded evidence. If data that was previously excluded is found necessary, the user must remove the related evidence item from the case, and then add the evidence again, using options that will include the desired data.

To set case evidence refining options

1. Click the *Evidence Refinement (Advanced)* icon in the left pane.
   The Evidence Refinement (Advanced) menu is organized into two dialog tabs:
   - **Refine Evidence by File Status/Type**
   - **Refine Evidence by File Date/Size**
2. Click the corresponding tab to access each dialog.
3. Set the needed refinements for the current evidence item.
4. To reset the menu to the default settings, click **Reset**.
5. To accept the refinement options you have selected and specified, click **OK.**

Refining Evidence by File Status/Type

Refining evidence by file status and type allows you to focus on specific files needed for a case.

Refine by File Status/Type Options

Options	Description
Include File Slack	Mark to include file slack space in which evidence may be found.
Include Free Space	Mark to include unallocated space in which evidence may be found.
Include KFF Ignorable Files	(Recommended) Mark to include files flagged as ignorable in the KFF for analysis.
Include OLE Streams and Office 2007 package contents	Mark to include Object Linked and Embedded (OLE) data streams, and Office 2007 (DOCX, and XLSX) file contents that are layered, linked, or embedded.
Deleted	Specifies the way to treat deleted files. Options are: ● Ignore Status ● Include Only ● Exclude Defaults to “Ignore Status.”
Encrypted	Specifies the way to treat encrypted files. Options are: ● Ignore Status ● Include Only ● Exclude Defaults to “Ignore Status.”
From Email	Specifies the way to treat email files. Options are: ● Ignore Status ● Include Only ● Exclude Defaults to “Ignore Status.”
File Types	Specifies which types of files to include and exclude.
Only add items to the case that match both File Status and File Type criteria	Applies selected criteria from both File Status and File Types tabs to the refinement. Will not add items that do not meet all criteria from both pages. If this option is not checked, and if you set a File Status, such as From Email > Include Only, then only the File Status value will be used and the File Type will be ignored.

Refining Evidence by File Date/Size

Refine evidence further by making the addition of evidence items dependent on a date range or file size that you specify. However, once in the case, filters can also be applied to accomplish this.

Refine by File Date/Size Options

Exclusion	Description
Refine Evidence by File Date	To refine evidence by file date: 1. Check *Created*, *Last Modified*, and/or *Last Accessed*. 2. In the two date fields for each date type selected, enter beginning and ending date ranges.
Refine Evidence by File Size	To refine evidence by file size: 1. Check *At Least* and/or *At Most* (these are optional settings). 2. In the corresponding size boxes, specify the applicable file size. 3. In the drop-down lists, to the right of each, select *Bytes*, *KB*, or *MB*.

Selecting Index Refinement (Advanced) Options

The Index Refinement (Advanced) feature allows you to specify types of data that you do not want to index. You may choose to exclude data to save time and resources, or to increase searching efficiency.

Note: AccessData strongly recommends that you use the default index settings.

To refine an index

1. Within the *Detailed Options* dialog of the *New Case* wizard, click **Index Refinement (Advanced)** in the left pane.

   The Index Refinement (Advanced) menu is organized into two dialog tabs:

   - **Refine Index by File Status/Type**
   - **Refine Index by File Date/Size**
2. Click the corresponding tab to access each dialog.
3. Define the refinements you want for the current evidence item.
4. Click *Reset* to reset the menu to the default settings.
5. Click **OK** when you are satisfied with the selections you have made.

Refining an Index by File Status/Type

Refining an index by file status and type allows the investigator to focus attention on specific files needed for a case through a refined index defined in a dialog.

At the bottom of the two Index Refinement tabs you can choose to mark the box for **Only index items that match both File Status AND File Types criteria**, if that suits your needs.

Refine Index by File Status/Type Options

Options	Description
Include File Slack	Mark to include free space between the end of the file footer, and the end of a sector, in which evidence may be found.
Include Free Space	Mark to include both allocated (partitioned) and unallocated (unpartitioned) space in which evidence may be found.
Include KFF Ignorable Files	Mark to include files flagged as ignorable in the KFF for analysis.
Include Message Headers	Marked by default. Includes the headers of messages in filtered text. Unmark this option to exclude message headers from filtered text.
Do not include document metadata in filtered text	Not marked by default. This option lets you turn off the collection of internal metadata properties for the indexed filtered text. The fields for these metadata properties are still populated to allow for field level review, but the you will no longer see information such as Author, Title, Keywords, Comments, etc in the Filtered text panel of the review screen. If you use an export utility such as ECA or eDiscovery and include the filtered text file with the export, you will also not see this metadata in the exported file.
Include OLE Streams	Includes Object Linked or Embedded (OLE) data streams that are part of files that meet the other criteria.
Deleted	Specifies the way to treat deleted files. Options are: ● Ignore status ● Include only ● Exclude
Encrypted	Specifies the way to treat encrypted files. Options are: ● Ignore status ● Include only ● Exclude
From Email	Specifies the way to treat email files. Options are: ● Ignore status ● Include only ● Exclude
Include OLE Streams	Includes Object Linked or Embedded (OLE) files found within the evidence.
File Types	Specifies types of files to include and exclude.
Only add items to the Index that match both File Status and File Type criteria	Applies selected criteria from both File Status and File Types tabs to the refinement. Will not add items that do not meet all criteria from both pages.

Refining an Index by File Date/Size

Refine index items dependent on a date range or file size you specify.

Refine Index by File Date/Size Options

Exclusion	Description
Refine Index by File Date	To refine index content by file date: 1. Select **Created**, **Last Modified**, or **Last Accessed**. 2. In the date fields, enter beginning and ending dates within which to include files.
Refine Index by File Size	To refine evidence by file size: 1. Click in either or both of the size selection boxes. 2. In the two size fields for each selection, enter minimum and maximum file sizes to include. 3. In the drop-down lists, select whether the specified minimum and maximum file sizes refer to *Bytes*, *KB*, or *MB*.

Selecting Lab/eDiscovery Options

This option is available for those with AD Lab and Summation licenses.

AD Lab and eDiscovery have additional options available for advanced de-duplication analysis.

De-duplication is separated by email items and non-email items. Within each group, the available options can be applied by case or by Custodian.

Note: This option is not enabled by default when using the eDiscovery Default processing profile.

The following table provides more information regarding each option and its description.

AD Lab/eDiscovery Detailed Options

Option	Description
Enable Advanced De-duplication Analysis	
Email Items	*De-duplication Scope*
	Choose whether you want this de-duplication process to be applied at the Case level, or at the Custodian level. • Case Level • People (Custodian) Level

AD Lab/eDiscovery Detailed Options (Continued)

Option	Description

	De-duplication Options
	For each item type you check, AD Lab eliminates duplicates from the case as it processes through the collected evidence. Uncheck an item type to keep all duplicate instances in your case.
	Available item types
	● Email To
	● Email From
	● Email CC
	● Email BCC
	● Email Subject
	● Email Submit Time
	● Email Delivery Time
	● Email Attachment Time
	● Email Attachment Count
	● Email Hash
	  ■ Body Only
	  ■ Body and Attachments

Non-email Items	*De-duplication Scope*
	Choose whether you want this de-duplication process to be applied to the entire case or at the custodian level. ● Case Level ● People (Custodian) Level
	De-duplication Option There is only one option available for non-email items; either you are going to de-duplicate just the actual files, or if unmarked, you will de-duplicate actual files only, or all files, including children, zipped, OLE, and carved files.
	● Actual Files Only
Propagate Email Attributes	When an email has attachments or OLE items, marking this option causes the email's attributes to be copied and applied to all "child" files of the email "parent."
Cluster Analysis	Invokes the extended analysis of documents to determine related, near duplicates, and email threads. See Viewing Data in Volume Shadow Copies on page 369. Configure the details by clicking **NDA Options**.
Cluster Analysis Options	This lets you specify the options for Cluster Analysis. You can specify which document types to process: ● Documents ● Presentations ● Spreadsheets ● Email You can also specify the similarity threshold, which determines the level of similarity required for documents to be considered related or near duplicates.

AD Lab/eDiscovery Detailed Options (Continued)

Option	Description
Include Extended Information in the Index	If you create a case in FTK and are going to review it in Summation or eDiscovery, select this option to make the index data fully compatible with Summation/ eDiscovery.
Enable 'Standard Viewer'	If you create a case in FTK and are going to review it in Summation or eDiscovery, select this option to automatically create a set of SWF files for all document files found during processing. These SWF files will be used as the default file rather than the original file when annotating and redacting within the case and will be created during processing for any file 1 MB or larger. Smaller files will be created on-the-fly when selected in Review. When opened in the Standard Viewer in eDiscovery or Summation, the converted SWF file is displayed by default, rather than the original file. This enables users to work on a file without first having to manually create a SWF file. **Note:** This option is disabled by default, and when enabled, slows processing speeds.
Create Email Threads	Sorts and groups emails by conversation threads.

Adding Evidence to a New Case

If you marked Open the Case before clicking **OK** in the *New Case Options* dialog, when case creation is complete, the *Examiner* opens. Evidence items added here will be processed using the options you selected in pre-processing, unless you click *Refinement Options* to make changes to the original settings.

Working with Volume Shadow Copies

You can examine data that is contained in NTFS Volume Shadow Copies.

See Examining Data in Volume Shadow Copies on page 147.

Converting a Case from Version 2.2 or Newer

If you have cases that were created in version 2.2 or later, you can convert them to the latest version. Refer to the following guidelines for migrating 2.x cases.

Important: Consider the following information:

- Any case created with a version prior to 2.2 must be re-processed completely in the latest version.
- AccessData recommends reprocessing active cases instead of attempting to convert them, to maximize the features and capabilities of the new release.
- AccessData recommends that no new evidence be added to any case that has been converted from an earlier version. This is because newer versions of processing gathers more information than was done in versions prior to 2.x.

  Therefore, if evidence is added to a converted 2.2 case, the new evidence will have all the info gathered by the newest version; however, the data from the converted 2.2 case will not have this additional information. This may cause confusion and bring forensic integrity into question in a court of law.

For more information, see the webinar that explains Case Portability in detail. This webinar can be found under the Core Forensic Analysis portion of the webpage: http://www.accessdata.com/Webinars.

The AccessData website works best using Microsoft Windows Explorer. You will be required to create a username and password if you have not done so in the past. If you have used this website previously, you will need to verify your email address. The website normally remembers the rest of the information you enter.

For instructions on converting cases, see the Migrating Cases document located at

http://www.accessdata.com/support/product-downloads/ftk-download-page

Chapter 6

Managing Case Data

This chapter includes the following topics

- Backing Up a Case (page 109)
- Archiving and Detaching a Case (page 112)
- Attaching a Case (page 113)
- Restoring a Case (page 114)
- Migrating Cases Between Database Types (page 115)

Backing Up a Case

About Performing a Backup and Restore on a Multi-Box Installation

If you have installed the Examiner and the database on separate boxes, or if you have case folders on a different box than the applicaiton, there are special considerations you must take into account. For instructions on how to back up and restore in this environment, see Configuring a Multi-box Setup in the *User Guide*.

Performing a Backup of a Case

At certain milestones of an investigation, you should back up your case to mitigate the risk of an irreversible processing mistake or perhaps case corruption.

Case backup can also be used when migrating or moving cases from one database type to another. For example, if you have created cases using 4.1 in an Oracle database and you want to upgrade to 5.0.x and migrate the case(s) to a PostgreSQL database. Another example is if you have created cases using 5.0.x in an Oracle database and you want to move the case(s) to the same version that is running a PostgreSQL database.

When you back up a case, the case information and database files (but not evidence) are copied to the selected destination folder. AccessData recommends that you store copies of your drive images and other evidence separate from the backed-up case.

Important: Case Administrators back up cases and must maintain and protect the library of backups against unauthorized restoration, because the user who restores an archive becomes that case's administrator.

Note: Backup files are not compressed. A backed-up case requires the same amount of space as that case's database table space and the case folder together.

Starting in 4.2, all backups are performed using the database independent format rather than a native format. The database independent format facilitates migrating and moving cases to a different database application or version. You can perform a backup using a native format using the dbcontrol utility. For more information, contact AccessData Technical Support.

Important: Do not perform a backup of a case while any data in that case is being processed.

To back up a case

1. In the *Case Manager* window, select the case to back up. You can use Shift + Click, or Ctrl + Click to select multiple cases to backup.
2. Do one of the following:
   - Click **Case > Backup > Backup**.
   - Right-click on the case in the *Cases* list, and click **Backup**.
3. In the field labeled *Backup folder*, enter a destination path for the backup files.

   Important: Choose a folder that does not already exist. The backup will be saved as a folder, and when restoring a backup, point to this folder (not the files it contains) in order to restore the case.
4. If you are using 4.1 to backup a case in order to migrate it to 4.2, make sure that you select **Use database independent format**.

   In 4.2, all backups are performed using the database independent format.

5. (Optional) Back up the Summation or Resolution1 application database.

   If you have a licence for Summation or Resolution1, when you back up a case, you can also select to backup the Summation or Resolution1 application database by doing the following:

   5a. Click **App DB...**.

   5b. Specify the App DB properties and credentials.

6. Click **OK**.

Note: The following information may be useful:

- Each case you back up should have its own backup folder to ensure all data is kept together and cannot be overwritten by another case backup. In addition, AccessData recommends that backups be stored on a separate drive or system from the case, to reduce space consumption and to reduce the risk of total loss in the case of catastrophic failure (drive crash, etc.).
- The absolute path of the case folder is recorded. When restoring a case, the default path is the original path. You can choose the default path, or enter a different path for the case restore.

Performing a Database-only Backup

There is a new *-backuponly* switch that you can use with DBControl.exe that will only backup the database portion of the case, but does not backup the case folder.

To perform a database-only backup

1. Open a *Command Prompt* in Windows.
2. Go to the following path:

   C:\Program Files\AccessData\Forensic Toolkit*version*\bin
3. Enter the following:

   dbcontrol.exe pgdb=adg port=<port#> -backuponly caseid=<case#> backuppath=<path to backup the db>

Note: You will need to have the port number, case ID, and backup path before you begin the database-only backup process.

Archiving a Case

When work on a case is completed and immediate access to it is no longer necessary, that case can be archived.

The Archive and Detach function copies that case's database table space file to the case folder, then deletes it from the database. This prevents two people from making changes to the same case at the same time, preserving the integrity of the case, and the work that has been done on it. Look for filename DB fn. Archive keeps up to four backups, DB f0, DB f1, DB f2, and DB f3.

To archive a case

1. In the *Case Manager*, select the case to archive.
2. Click **Case > Backup > Archive**.
3. A prompt asks if you want to use an intermediate folder.

   The processing status dialog appears, showing the progress of the archive. When the archive completes, close the dialog.

To view the resulting list of backup files

1. Open the cases folder.

   Note: The cases folder is no longer placed in a default path; instead it is user-defined.

2. Find and open the sub-folder for the archived case.
3. Find and open the sub-folder for the archive (DB fn).
4. You may view the file names as well as Date modified, Type, and Size.

Archiving and Detaching a Case

When work on a case is not complete, but it must be accessible from a different computer, archive and detach that case.

The Archive and Detach function copies that case's database table space file to the case folder, then deletes it from the database. This prevents two people from making changes to the same case at the same time, preserving the integrity of the case, and the work that has been done on it.

To archive and detach a case

1. In the *Case Manager*, click **Case > Backup > Archive and Detach**.
   The case is archived.
2. You will see a notice informing you that the specified case will be removed from the database. Click **OK** to continue, or **Cancel** to abandon the removal and close the message box.
3. A prompt asks if you want to use an intermediate folder.
   The processing status dialog appears, showing the progress of the archive. When the archive completes, close the dialog.

To view the resulting list of files

1. Open the folder for the archived and detached cases.
2. Find and open the sub-folder for the archived case.

   Note: The cases folder is no longer placed in a default path; instead it is user-defined.

3. Find and open the sub-folder for the archive (DB fn).

You may view the file names as well as Date Modified, Type, and Size.

Attaching a Case

Attaching a case is different from restoring a case. You would restore a case from a backup to its original location in the event of corruption or other data loss. You would attach a case to the same or a different machine/ database than the one where it was archived and detached from.

The Attach feature copies that case's database table space file into the database on the local machine.

Note: The database must be compatible and must contain the AccessData schema.

To attach a detached case

1. Click **Case > Restore > Attach**.

Important: Do NOT use "Restore" to re-attach a case that was detached with "Archive." Instead, use "Attach." Otherwise, your case folder may be deleted.

2. Browse to and select the case folder to be attached.
3. (Optional) Select **Specify the location of the DB files** and browse to the path to store the database files for this case.

   3a. Select **In the case folder** to place the database files in subfolderof the case folder.

4. Click **OK**.

Restoring a Case

When your case was backed up, it was saved as a folder. The folder selected for the backup is the folder you must select when restoring the backup.

Note: Do not use the *Restore...* function to attach an archive (instead use *Attach...*).

To restore a case

1. Open the *Case Manager* window.
2. Do either of these:
   - Click **Case > Restore > Restore**.
   - Right-click on the *Case Manager* case list, and click **Restore > Restore**.
3. Browse to and select the backup folder to be restored.
4. (Optional) Select **Specify the location of the DB files** and browse to the path to store the database files for this case.

   4a. Select **In the case folder** to place the database files in subfolderof the case folder.
5. You are prompted if you would like to specify a different location for the case folder. The processing status dialog appears, showing the progress of the archive. When the archive completes, close the dialog.

Deleting a Case

To delete a case from the database

1. In the *Case Manager* window, highlight the name of the case to be deleted from the database.
2. Do either of these:
   - Click **Case > Delete**.
   - Right-click on the name of the case to deleted, and click **Delete**
3. Click **Yes** to confirm deletion.

WARNING: This procedure also deletes the case folder. It is recommended that you make sure you have a backup of your case before you delete the case or else the case is not recoverable.

Storing Case Files

Storing case files and evidence on the same drive substantially taxes the processors' throughput. The system slows as it saves and reads huge files. For desktop systems in laboratories, you can increase the processing speed by saving evidence files to a separate server. For more information, see the separate installation guide.

If taking the case off-site, you can choose to compromise some processor speed for the convenience of having your evidence and case on the same drive, such as a laptop.

Migrating Cases Between Database Types

You can migrate or move cases from one database to another. For more information, see the *Quick Install Guide* and the *Upgrading Cases* guide.

Chapter 7

Working with Evidence Image Files

This chapter contains the following topics

- Verifying Drive Image Integrity (page 117)
- Mounting an Image to a Drive (page 118)
- Benefits of Image Mounting (page 118)
- Characteristics of a Logically Mounted Image (page 119)
- Characteristics of a Physically Mounted Image (page 119)
- Mounting an Image as Read-Only (page 119)
- Mounting a Drive Image as Writable (page 120)
- Unmounting an Image (page 121)
- Restoring an Image to a Disk (page 121)
- Performing Final Carve Processing (page 121)
- Recovering Processing Jobs (page 122)

Verifying Drive Image Integrity

A drive image can be altered or corrupted due to bad media, bad connectivity during image creation, or by deliberate tampering. This feature works with file types that store the hash within the drive image itself, such as EnCase (E01) and SMART (S01) images.

To verify an evidence image's integrity, a hash of the current file is generated and allows you to compare that to the hash of the originally acquired drive image.

To verify that a drive image has not changed

1. Select **Tools** > **Verify Image Integrity**.
   In case the image file does not contain a stored hash, one can be calculated. The Verify Image Integrity dialog provides the following information:

Column	Description
Image Name	Displays the filename of the evidence image to be verified.
Path	Displays the path to the location of the evidence image file.
Command	Click **Verify** or **Calculate** to begin hashing the evidence image file.

2. Click either **Calculate**, or **Verify** according to what displays in the Command column, to begin hashing the evidence file.

The *Progress* dialog appears and displays the status of the verification. If the image file has a stored hash, when the verification is complete, the dialog shows and compares both hashes. Completing these processes may take some time, depending on the size of the evidence, the processor type, and the amount of available RAM.

Mounting an Image to a Drive

Image Mounting allows forensic images to be mounted as a drive or physical device, for read-only viewing. This action opens the image as a drive and allows you to browse the content in Windows and other applications. Supported types are RAW/dd images, E01, S01, AD1, and L01.

Full disk images RAW/dd, E01, and S01 can be mounted Physically. Partitions contained within full disk images, as well as Custom Content Images of AD1 and L01 formats can be mounted Logically. The differences are explained in this section.

Note: Encrypted images cannot be mounted as either a drive or physical device.

Benefits of Image Mounting

The ability to mount an image with AccessData forensic products provides the following benefits:

- Mount a full disk image with its partitions all at once; the disk is assigned a Physical Drive name and the partitions are automatically assigned a drive letter beginning with either the first available, or any available drive letter of your choice.
- A full disk image mounted physically, and assigned a Physical Drive name that can be read using Imager or with any Windows application that performs Physical Name Querying.
- Mount images of multiple drives and/or partitions. The mounted images remain mounted until unmounted or until Imager is closed.
- Mounted images can be easily unmounted in any order, individually, or all at once.
- A logically mounted image may be viewed in Windows Explorer as though it were a drive attached to the computer, providing the following benefits:
  - File types with Windows associations can be viewed in their native or associated application, when that application is installed locally.
  - Anti-virus applications can be run on the mounted image.
  - Because the logically mounted image is seen as a drive in Windows Explorer, it can be shared, and viewed from remote computers when Remote Access has been configured correctly.
  - Files can be copied from the mounted image to another location.
- Mount NTFS / FAT partitions contained within images as writable block devices. This feature caches sections of a read-only image to a temporary location allowing the user to “write” to the image without compromising the integrity of the original image.

  Once mounted via the write cache mount method, the data can then be leveraged by any 3rd party tools which require write access.

Characteristics of a Logically Mounted Image

AD1 and L01 are both custom content images, and contain full file structure, but do not contain any drive geometry or other physical drive data. Thus, these images do not have the option of being mounted Physically.

Note: When Logically mounting an image, the drive or partition size displays incorrectly in the Windows **Start > Computer** view. However, when you open the “drive” from there, the folders and files contained within the mounted image do display correctly.

Characteristics of a Physically Mounted Image

When you mount an image physically, while it cannot be viewed by Windows Explorer, it can be viewed outside of Imager using any Windows application that performs Physical Name Querying.

E01, S01, and RAW/dd images are drive images that have the disk, partition, and file structure as well as drive data. A physical disk image can be mounted Physically; the disk image partitions can be mounted Logically.

Mounting an Image as Read-Only

To mount an image

1. If you already have the desired image added as evidence in the case, select that item, then do Step 2 to auto-populate the Source box with the image file to be mounted, as shown in Step 3.

   If you do not already have the desired image added as evidence, begin with Step 2.
2. Do one of the following:
   - Right-click and choose **Mount Image to Drive.**
   - Select the image from the Evidence tree. Right-click and choose **Mount Image to Drive**.
   - Click **Tools > Mount Image to Drive,** then browse to the image on your local drive or on a network drive you have access to.
3. Enter the path and filename, or click **Browse** to populate the Source box with the path and filename of the image to be mounted.

   After selecting an image, the Mount Type will default to the supported mapping based on the image type selected. Click the drop-down to display other available mount types. After selecting an image, the Map Type will default to the supported mapping based on the image type selected. Click the drop-down to display other available map types.
4. Select the Mount Type to use for mounting.

   Available Mount Types are Physical & Logical, Physical Only, and Logical Only.

   If the Mount Type selected includes Logical, you can select the Drive Letter to assign as the mount point.
5. Click the *Drive Letter* drop-down to see all drive letters that are available for assignment to the mounted image.
6. Click the *Mount Method* drop-down to select **Block Device / Read Only** or **File System / Read Only**.

Note: If you are mounting an HFS image of a Mac drive, you must choose **File System / Read Only** to view contents of the drive. Otherwise, it will appear empty, and may prompt you to format the drive.

7. Click **Mount**.

   All the related mount information will be displayed in the Mapped Image List.

   To mount another image, repeat the process. You can continue to mount images as needed, until you run out of evidence to add, or mount points to use. Mounted images remain available until unmounted, or until the program is closed.

8. Click **Close** to return to the main window.

Mounting a Drive Image as Writable

When mounting an image as writable, you must be working with a physical image, and the mount type you select must be Physical & Logical. This is the only option that provides the **Block Device /Writable** Mount Method.

To mount a drive image as writable

1. In the *Examiner*, click **Tools > Mount Image to Drive**.
2. Select a full disk image such as 001/Raw dd, E01, or S01 file type.
3. In the *Mount Type* drop-down, select **Physical & Logical**.
4. In the *Drive Letter* drop-down, select **Next Available** (default), or select a different drive letter.

Note: Check your existing mappings. If you map to a drive letter that is already in use, the original will prevail and you will not be able to see the mapped image contents.

5. In the *Mount Method* drop-down, select **Block Device / Writable**.
6. In the *Write Cache Folder* text box, type or click **Browse** to navigate to the folder where you want the Write Cache files to be created and saved.
7. Click **Mount.**

   You will see the mapped images in the Mapped Image List.

To view or add to the writable mapped drive image

1. On your Windows desktop, click **Start > Computer** (or **My Computer**).
2. Find the mapped drive letter in your Hard Disk Drives list. It should be listed by the name of the Image that was mounted, then the drive letter.
3. Double-click on it as you would any other drive.
4. As a test, right-click and choose **New > Folder.**
5. Enter a name for the folder and press **Enter**.
6. The folder you created is displayed in the Folder view.
7. Mapped images remain mapped until unmapped, or until the application is shut down.

Unmounting an Image

To unmount a mounted image

1. Click **File > Image Mounting.** The *Map Image to Drive* dialog opens.
2. Highlight the images to unmount, click **Unmount.** To unmount multiple mappings, click the first, then Shift-click the last to select a block of contiguous mappings. Click a file, then Ctrl-click individual files to select multiple non-contiguous mappings.)
3. Click **Done** to close the *Map Image to Drive* dialog.

Restoring an Image to a Disk

A physical image such as 001 (RAW/dd), E01, or S01, can be restored to a drive of equal or greater size to the original, un-compressed drive.

To restore an image to a disk

1. Connect a target drive to your computer.
2. In the *Examiner*, click **Tools > Restore Image to Disk**.
3. Click **Browse** to locate and select the source image. It must be a full-disk image such as 001 (Raw/dd), E01, or S01.

   The source image must be a disk image. A custom content image such as AD1 will not work for this feature.
4. Click the *Destination Drive* drop-down, select the target drive you connected in Step 1. If you do not see that drive in the list, click **Refresh**.
5. Mark the **Zero-fill remainder of destination drive** check box if the drive is larger than the original un-compressed drive.
6. Mark the **Notify operating system to rescan partition table when complete** check box to allow the new drive to be seen by the OS. If you plan to connect the drive in a different computer there is no need to do this step.

   When you are finished selecting options, click **Restore Image** to continue.

Performing Final Carve Processing

When you have selections saved as carved files from any file in the Hex viewer, performing Final Carve Processing carves the files, saves them, adds them to the case, and even creates or assigns them to bookmarks you specified when the data was selected.

Final Carve Processing jobs can be monitored in the Progress Window as Additional Analysis Jobs.

Recovering Processing Jobs

Jobs that are started but unable to finish for whatever reason can be deleted or restarted. Click **Tools > Recover Processing Jobs**. If no jobs remain unfinished, the *Recover Processing Jobs* dialog box is empty. Click **Close**. If there are jobs in the list, you can choose whether to Restart or Delete those jobs.

To recover incomplete processing jobs

1. Click **Select All**, **Unselect All**, or mark the check box for each job to be recovered.
2. Click **Restart**.
3. In the *Recovery Type* dialog, choose the recovery type that suits your needs:
   - **Continue processing** from where the job ended.
   - **Restart** the job from the beginning.
4. Click **Close**.
5. To verify the progress of a restarted or continued job, click **Tools > Show Progress Window**.

To remove incomplete processing jobs

1. Click **Select All**, **Unselect All**, or mark the check box for each job to discard.
2. Click **Delete**.
3. Click **Yes** to confirm that you want to delete the job permanently.
4. Click **Close**.

Chapter 8

Working with Static Evidence

This chapter includes the following topics

- Static Evidence Compared to Remote Evidence (page 123)
- Acquiring and Preserving Static Evidence (page 124)
- Adding Evidence (page 124)
- Working with Evidence Groups (page 128)
- Selecting Evidence Processing Options (page 129)
- Selecting a Language (page 130)
- Examining Data in Volume Shadow Copies (page 131)
- Using Additional Analysis (page 135)
- Data Carving (page 140)
- Hashing (page 140)
- Viewing the Status and Progress of Data Processing and Analysis (page 142)
- Viewing Processed Items (page 143)

Static Evidence Compared to Remote Evidence

Static evidence describes evidence that has been captured **to an image** before being added to the case.

Live evidence describes any data that is not saved **to an image** prior to being added to a case. Such evidence is always subject to change, and presents risk of data loss or corruption during examination. For example, a suspect's computer, whether because a password is not known, or to avoid the suspect's knowing that he or she is under suspicion, may be imaged live if the computer has not yet been or will not be confiscated.

Remote evidence describes data that is acquired from remote live computers in the network after the case has been created.

This chapter covers working with static evidence. For more information regarding acquisition and utilization of remote evidence, see Working with Live Evidence (page 144).

Acquiring and Preserving Static Evidence

For digital evidence to be valid, it must be preserved in its original form. The evidence image must be forensically sound, in other words, identical in every way to the original.

See also About Acquiring Digital Evidence (page 26)

Adding Evidence

When case creation is complete, the Manage Evidence dialog appears. Evidence items added here will be processed using the options you selected in pre-processing. Please note the following information as you add evidence to your case:

- You can now drag and drop evidence files from a Windows Explorer view into the *Manage Evidence* dialog.
- You can repeat this process as many times as you need to, for the number of evidence items and types you want to add.
- DMG (Mac) images are sometimes displayed as “Unrecognized File System.” This happens only when the files are not “Read/Write” enabled.

  If the DMG is a full disk image or an image that is created with the read/write option, then it is identified properly. Otherwise the contents will not be recognized properly.
- After processing, the Evidence Processing selected options can be found in the case log. You can also view them by clicking **Evidence > Add/Remove.** Double-click on any of the evidence items to open the *Refinement Options* dialog.
- Popular mobile phone formats (found in many MPE images) such as M4A, MP4, AMR, and 3GP can be recognized. These file types will play inside the Media tab as long as the proper codecs are installed that would also allow those files to play in Windows Media Player.

To add static evidence (an exact image, or “snapshot” of electronic data found on a hard disk or other data storage device) to an existing case, select **Evidence > Add/Remove** from the menu bar and continue.

Note: Use Universal Naming Convention (UNC) syntax in your evidence path for best results.

Click **Refinement Options** to override settings that were previously selected for evidence added to this case. If you do not click **Refinement Options** here, the options that were specified when you created the case will be used.

Configuring Default Processing Options for a Case (page 76)

After evidence has been added, you can perform many processing tasks that were not performed initially. Additional evidence files and images can be added and processed later, if needed.

Manage Evidence Options

Option	Description
Add	Opens the *Select Evidence Type* dialog. Click to select the evidence type, and a Windows Explorer instance will open, allowing you to navigate to and select the evidence you choose.
Remove	Displays a caution box and asks if you are sure you want to remove the selected evidence item from the case. Removing evidence items that are referenced in bookmarks and reports will remove references to that evidence and they will no longer be available. Click **Yes** to remove the evidence, or click **No** to cancel the operation.
Display Name	The filename of the evidence being added.
State	The State of the evidence item: ● " " (empty) Indicates that processing is complete. ● "+" Indicates the item is to be added to the case ● "–" Indicates the item is to be removed from the case. ● "*" Indicates the item is processing. ● "!" Indicates there was a failure in processing the item. If you click **Cancel** from the *Add Evidence* dialog, the state is ignored and the requested processing will not take place. **Note:** If the *State* field is blank and you think the item is still processing, from any tab view, click **View > Progress Window** to verify.
Path	The full pathname of the evidence file. **Note:** Use universal naming convention (UNC) syntax in your evidence path for best results.
ID/Name	The optional ID/Name of the evidence being added.
Description	The options description of the evidence being added. This can be the source of the data, or other description that may prove helpful later.
Evidence Group	Click the drop-down to assign this evidence item to an Evidence Group. For more information regarding Evidence Groups, see Working with Evidence Groups (page 128).
Time Zone	The time zone of the original evidence. Select a time zone from the drop-down list.
Merge Case Index	Merges fragmented index segments to improve performance of index-related commands, such as Index Searching. **Note:** The application automatically merges the case index when system resources allow whether or not *Merge Case Index* is selected. Selecting this option forces the merge to execute regardless of system resources.
Language Setting	Select the code page for the language to view the case in. The *Language Selection* dialog contains a drop-down list of available code pages. Select a code page and click **OK**.
Case KFF Options	Opens the KFF Admin box for managing KFF libraries, groups, and sets for this case.

Manage Evidence Options (Continued)

Option	Description
Refinement Options	Displays the Refinement Options for Evidence Processing. This dialog has limited options compared to the Refinement Options selectable prior to case creation. Select the options to apply to the evidence being added, then click **OK** to close the dialog. Configuring Default Processing Options for a Case (page 76)

When you are satisfied with the evidence options selected, click **OK**.

Note: To remove evidence from the list either before processing, or after it has been added to the case, select the evidence item in the list, then click **Remove**.

Note: When you export data from a case as an image, and then add that image as evidence in either the same case or a different case, the name of the image is renamed using a generic term. This prevents a user generated image name from being indexed with evidence.

To add new evidence to the case

1. Do one of the following:
   - Drag and drop the evidence file into the **Manage Evidence > Evidence Name** list field.
   - Click **Add** to choose the type of evidence items to add into a new case.

   Important: Consider the following:
   - Evidence taken from any physical source that is removable, whether it is a “live” drive or an image, will become inaccessible to the case if the drive letters change or the evidence-bearing source is moved. Instead, create a disk image of this drive, save it either locally, or to the drive you specified during installation, then add the disk image to the case. Otherwise, be sure the drive will be available whenever working on the case.
   - To add physical or logical drives as evidence on any 64-bit Windows system you must run the application as an Administrator. Otherwise, an empty drive list displays. If you encounter this problem on a 64-bit system, log out, then run again as Administrator.
   - While it is possible to add a CUE file as a valid image type, when adding a CUE file as “All images in a directory”, although adding the BIN and the CUE are actually the same thing the user gets double of everything.

     Workaround: Remove duplicates before processing.
2. Mark the type of evidence to add, and then click **OK**.
3. Click the **Browse** button at the end of the *Path* field to browse to the evidence folder. Select the evidence item from the stored location.
4. Click **OK**.

   Note: Folders and files not already contained in an image when added to the case will be imaged in the AD1 format and stored in the case folder. If you select AD1 as the image type, you can add these without creating an image from the data.
5. Fill in the ID/Name field with any specific ID or Name data applied to this evidence for this case.
6. Use the Description field to enter an optional description of the evidence being added.
7. Select the **Evidence Group** that this evidence item belongs to. Click **Manage** to create and manage evidence groups.

8. Select the **Time Zone** of the evidence where it was seized from the drop-down list in the **Time Zone** field. This is required to save the added evidence.

   After selecting an Evidence Type, and browsing to and selecting the evidence item, the selected evidence displays under Display Name. The Status column shows a plus (+) symbol to indicate that the file is being added to the case.

To pause evidence processing

- In the Data Processing Status window, select the **Pause** button.

  An entry will appear in the Messages box stating that the processing has been paused and listing the date and time it was paused.

To resume evidence processing

- In the Data Processing Status window, select the **Resume** button.

  An entry will appear in the Messages box stating that the processing has resumed and listing the date and time it resumed.

Working with Evidence Groups

Evidence Groups let you create and modify groups of evidence. You can share groups of evidence with other cases, or make them specific to a single case.

To create an evidence group

1. In *Examiner*, click **Evidence > Add/Remove**.
2. With an evidence item selected in the *Display Name* box, click **Manage** to the right of Evidence Group.
3. In the *Manage Evidence Group* dialog, click **Create New** to create a new Evidence Group.
4. Provide a name for the new evidence group, and mark the **Share With Other Cases** box to make this group available to other cases you may be working on.
5. Click **Create** to create and save this new group.
6. Click **Close**.

To modify an evidence group

1. In *Examiner*, click **Evidence > Add/Remove**.
2. With an evidence item selected in the *Display Name* box, click **Manage** to the right of Evidence Group.
3. To modify a group, highlight it in the list, and click **Modify**.
4. Make the changes to the group, then click **Update**.
5. Click **Close**.

To delete an evidence group

1. In *Examiner*, click **Evidence > Add/Remove**.
2. With an evidence item selected in the *Display Name* box, click **Manage** to the right of Evidence Group.
3. To delete a group, highlight it in the list, and click **Delete**.
4. Click **Close**.

Selecting Evidence Processing Options

The Evidence Processing options allow selection of processing tasks to perform on the current evidence. Select only those tasks that are relevant to the evidence being added to the case.

See Configuring Default Processing Options for a Case on page 76.

After processing, the Evidence Processing options selected for this case can be found in the case log. You can also view them by clicking **Evidence > Add/Remove**. Double-click on any of the evidence items to open the *Refinement Options* dialog.

Some pre-processing options require others to be selected. For example:

- Data Carving depends on Expand
- KFF depends on MD5 hashing
- Flag Duplicates depends on MD5 hashing
- Indexing depends on Identification
- Flag bad extension depends on File Signature Analysis.

Different processing options can be selected and unselected depending on the specific requirements of the case.

At the bottom of every Refinement Options selection screen are the following options:

- *OK*: accepts current settings without saving for future use.
- *Cancel*: cancels the entire Detailed Options dialog without saving settings or changes, and returns to the New Case Options dialog.

If you choose not to index in the Processing Options page, but later find a need to index the case, click **Evidence > Additional Analysis**. Choose **All Items**, and check **dtSearch*** **Index**.

To set Evidence Refinement Options for this case

1. Click **Refinement Options** to open the *Refinement Options* dialog. Refinement Options are much the same as Detailed Options.

   The sections available are:

   - *Evidence Processing:* For more information on Evidence Processing options, see Selecting Evidence Processing Options (page 129).
   - *Evidence Refinement (Advanced)*: For more information on Evidence Refinement (Advanced) options, see Configuring Evidence Refinement (Advanced) Options (page 100).
   - *Index Refinement (Advanced)*: For more information on Index Refinement (Advanced), see Selecting Index Refinement (Advanced) Options (page 102).
2. Click **OK** to accept the settings and to exit the *Manage Evidence* dialog.
3. Select the **KFF Options** button to display the *KFF Admin* dialog.

   Note: The AD Alert and the AD Ignore Groups are selected by default.
4. Click **Done** to accept settings and return to the *Manage Evidence* dialog.
5. Click **Language Settings** to select the code page for the language to be used for viewing the evidence. More detail is given in the following section.
6. Click **OK** to add and process the evidence.

Selecting a Language

If you are working with a case including evidence in another language, or you are working with a different language Operating System, click **Language Settings** from the *Manage Evidence* dialog.

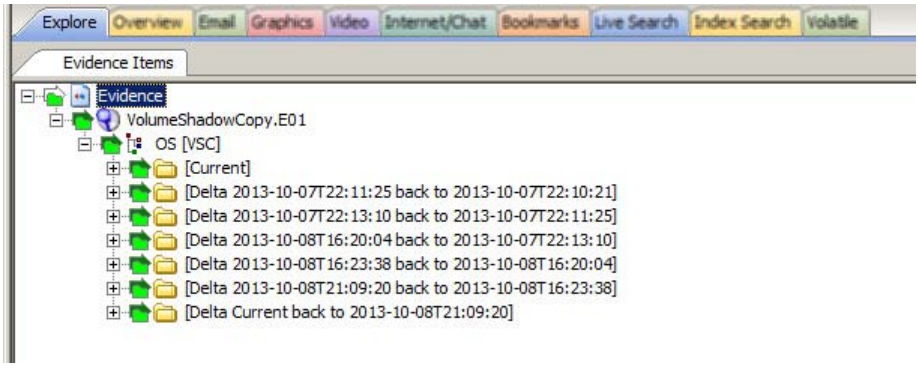
The *Language Setting* dialog appears, allowing you to select a code page from a drop-down list. When the setting is made, click **OK**.

Examining Data in Volume Shadow Copies

You can examine data that is contained in NTFS Volume Shadow Copies. In NTFS partitions, the Volume Shadow Copy Service (VSS) maintains a copy of every 16 KB block that is changed. These blocks are packaged up at predetermined times (which differ depending on the operating system being run) as a Volume Shadow Copy (VSC) or restore point. These restore points can contain data that has been renamed or deleted. They can also contain hidden malware, especially persistent code.

Encrypted drives are supported.

You can mount and process restore points as a separate evidence items within a case. When restore points are processed, a unique file system image for each restore point is created under the source NTFS partition.



You can view the files in the different file system images to analyze the difference between each restore point and the files that are unique to each one. This helps you see how a system has changed over a period of time. You can identify and parse files within the restore points and can search for evidence or malware hidden there.

You configure the processing of restore points when you add new evidence to a case. You can do this for a new case or an existing case. If the evidence that you are adding contains an NTFS partition with Volume Shadow Copy restore points, a *Select Restore Points* option is available. You can view all of the available restore points and select the ones that you want to process.

When viewing the restore point data, you can use the following VSC-related columns the provides details about the data.

VSC-related Columns

VSC-Delta Restore Point End	Date of second restore point of a delta file
VSC-Delta Restore Point Start	Date of first restore point of a delta file
VSC-Delta State	The state of a delta file as compared in two restore points
VSC-Renamed From	The name this file was renamed from
VSC-Renamed To	The name this file was renamed to
VSC- Restore Point Date	Date of restore point this file came from

See Managing Columns on page 481.

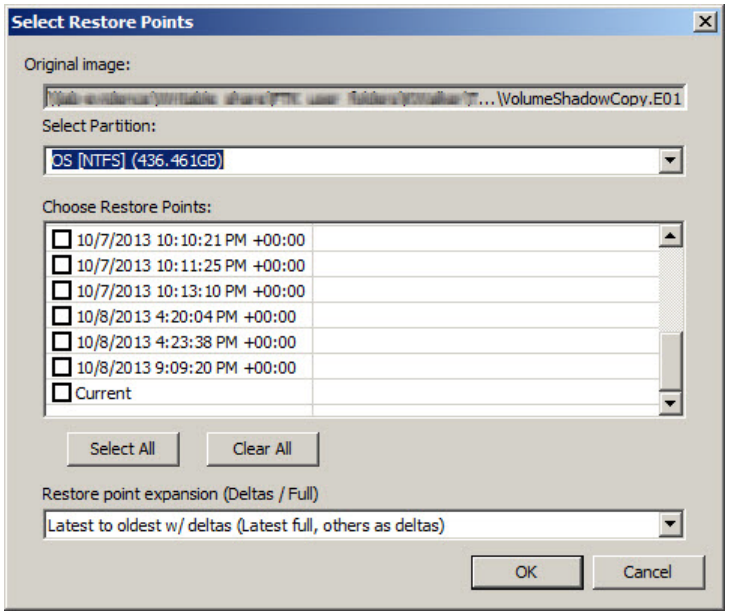
About Restore Point Processing Options

When you select restore points to process, you select the following options:

- Which restore points to include
- The restore point expansion options (Delta/Full)

Restore Points Selection

If an NTFS partition has restore points, you can select which restore points to to expand as file system images. Each restore point that you select is represented by a unique file system. You can select the *Current* files as well as any previous restore points.



Important: You can select to process one or more restore point. If you do not select a restore point, you cannot add it later within the same evidence item. You must re-add the NTFS partition as a new evidence item and then select the desired restore points.

Restore Point Expansion Options

You choose from the following expansion options.

Full	All restore points are added as full file systems. The benefit of this option is that you can view all of the files in all of the restore points. However, you will potentially have duplicate files, making the data set large. It can also make it more difficult to find the files that have been deleted or modified. If "Full" restore option is selected, you are warned if more than one restore point is checked. You can add the evidence item again if you don't choose to add it as a restore point image originally. You can then choose restore points.

Delta - Oldest to latest	Instead of creating a full partition for each restore point, one full partition is created for the oldest restore point selected while all newer restore points are created as deltas. The advantage of this option is that you do not have duplicate files and the contents of the other restore points are smaller, making it is easier to find the files or folders that have been deleted or modified.
Delta - Latest to Oldest	The latest restore point selected is created as a full image while all older restore points are created as deltas.

Managing Restore Points

To process restore point file systems

1. In either a new or an existing case, add new evidence, and select evidence that has an NTFS partition.
2. On the *Manage Evidence* page, click **Choose Restore Points**.

   If the button is active, then the evidence has an NTFS partition.

   If the button is grayed out, the evidence does not have an NTFS partition.

   When you click the button, if the NTFS partition does not have any restore points, a message is displayed.
3. Select the restore points that you want to process as file systems.

   See About Restore Point Processing Options on page 132.
4. Select the expansion option.
5. Click **OK**.

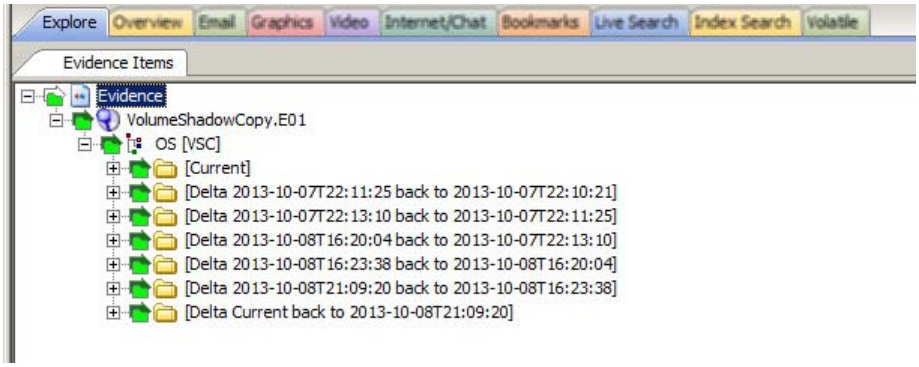
Viewing Restore Point Data

After the evidence with the restore points has been processed, you can view the data. You can view the created file systems for the restore points that you selected.

You can also add columns to the File List to display

To view restore point file systems

1. In the Examiner, click the **Explore** tab.
2. Select the evidence item and the the NTFS partition.
3. You can view a file system image for each restore point.



4. You can view the content of each restore point to compare folders and files.

5. You can use VSC-related columns to view detailed data.
   See VSC-related Columns on page 131.
6. You can also use searches, filters, and so on to find and analyze the files in the share points.

Note: If you selected “Latest to Oldest”, the tree will show *Current* first, but then the deltas are sorted by the oldest to the newest. If you selected “Oldest to Latest” the folders are sorted in the correct order.

Using Additional Analysis

After evidence has been added to a case and processed, you may wish to perform other analysis tasks. To further analyze selected evidence, click **Evidence** > **Additional Analysis**.

Most of the tasks available during the initial evidence processing remain available with Additional Analysis.

See Evidence Processing Options on page 82.

Specific items can also be targeted. Multiple processing tasks can be performed at the same time.

Make your selections based on the information in the table below. Click **OK** when you are ready to continue.

Additional Analysis Options

Field Item	Description	
Hashing / Job Options Tab		
File Hashes	These options create file hashes for the evidence. The Options are:	
	MD5 Hash:	This hash option creates a digital fingerprint based on the contents of the file. This fingerprint can be used to verify file integrity and to identify duplicate files.
	SHA-1 Hash:	This hash option creates a digital fingerprint based on the contents of the file. This fingerprint can be used to verify file integrity and to identify duplicate files.
	SHA-256:	This hash option creates a digital fingerprint based on the contents of the file. This fingerprint can be used to verify file integrity and to identify duplicate files.
	Flag Duplicates:	Mark to flag duplicate files. This applies to all files in the case, regardless of the Target Items selected.
	Note: A blank hash field appears for unallocated space files, the same as if the files had not been hashed at all. To notate in the hash field the reason for it being blank would slow the processing of the evidence into the case.	
KFF	Enables the Known File Filter (KFF) that lets you identify either known insignificant files that you can ignore or known illicit or dangerous files that you want to be alerted to. When you enable KFF, you must select a KFF Template to use. You can select an existing KFF Template from the drop-down menu or click **...** to create a new one. See Using the Known File Filter (KFF) on page 264. You can select to **Recheck previously processed items** when searching for new information, or when a KFF group is added or changed. Mark **Recheck previously processed items** if changes have been made to the KFF since the last check.	
Target Items	Select the items on which to perform the additional analysis. Highlighted, and Checked items will be unavailable if no items in the case are highlighted or checked. The following list shows the available options:	
	Highlighted Items:	Performs the additional analysis on the items highlighted in the File List pane when you select Additional Analysis.

Additional Analysis Options (Continued)

Field Item	Description	
	Checked Items:	Performs the additional analysis on the checked evidence items in the File List pane when you select Additional Analysis.
	Currently Listed Items:	Performs the additional analysis on all the evidence items currently listed in the File List pane when you select Additional Analysis.
	All Items:	Performs the additional analysis on all evidence items in the case.
PhotoDNA	Enables PhotoDNA which lets you compare images in your evidence against known images in a library. See Using PhotoDNA to Compare Images on page 322.	
Refinement	Include OLE Streams: Includes Object Linked or Embedded (OLE) items that are part of files that meet the other criteria.	
Job Options	Send Email Alert on Job Completion: Opens a text box for the entry of an email address destination for a notification email when these jobs complete. **Note:** Outgoing TCP traffic must be allowed on port 25. **Important!** These Emails are often filtered into Spam folders.	
Indexing / Tools tab		
Indexed Search	*dtSearch® Index*	Choose *dtSearch® Index* to create a dtSearch index that enables instantaneous index searches. Marking **dtSearch Index** activates the Entropy Test check box.
	Entropy Test	Select *Entropy Test* to exclude compressed or encrypted items from the indexing process.
Decryption	*Decrypt Credant Files:*	See Decrypting Credant Files (Dell Data Protection | Encryption Server) on page 194. If you select to decrypt Credant files, the *File Signature Analysis* option will automatically be selected as well.
	Perform Automatic Decryption:	Attempts to decrypt files using a list of passwords that you provide See Decrypting Files Using Right-Click Auto Decryption on page 187.
Other Tools:		
	Optical Character Recognition:	Parses text from graphics images and adds them to the Index. Creates an additional file with the OCR extension. Click **OCR Options** to select specific graphics files to run the OCR process on, or to set limiting factors such as size, or grayscale. For more detailed information regarding OCR settings and options, see Running Optical Character Recognition (OCR) (page 95).

Additional Analysis Options (Continued)

Field Item	Description	
	Explicit Image Detection:	Enables EID Options button. The EID license is purchased separately. This item will be disabled unless the license is detected on your CmStick. Click **EID Options** to select the processes to run. Choose default, speed, or accuracy settings. See Evaluating Explicit Material on page 319.
	Registry Reports:	Enables Registry Summary Reports (RSRs) to be used directly from Registry Viewer if it is installed. Click RSR Directory to specify the location of any RSR templates you have saved or downloaded from the AccessData web site.
	Cerberus Analysis	Performs a malware analysis on executable binaries. See About Cerberus Malware Analysis on page 212. See Running Cerberus Malware Analysis on page 230.
	Cerberus Analysis:	Lets you run the add on module for Cerberus Malware Triage. You can click *Cerberus Options* to access additional options. For more information see About Cerberus Malware Analysis (page 212)
	Language Identification	Analyzes the first two pages of every document to identify the languages contained within. The user will be able to filter by a Language field within review and determine who needs to review which documents based on the language contained within the document. See Identifying Document Languages on page 343.
	Document Content Analysis	Analyzes the content and groups it according to topic in the *Overview* tab. When selected, the DCA Options button is also activated and opens the Document Content Analysis Options. See Using Document Content Analysis on page 424.
	Entity Extraction (Document Content)	Identifies and extracts specific types of data in your evidence. You can select to process one or all of the following types of entity data: • Credit Card Numbers • Phone Numbers • Social Security Numbers In the *Examiner*, under the *Document Content* node in the *Overview* tab, you can view the extracted data. See Using Entity Extraction on page 420.
	Cluster Analysis	(AD Lab and Summation license only) Invokes the extended analysis of documents to determine related, near duplicates, and email threads. See Performing Cluster Analysis on page 426. Configure the details by clicking **Analysis Options**.

Additional Analysis Options (Continued)

Field Item	Description	
	Cluster Analysis Options	(AD Lab and Summation license only) This lets you specify the options for Cluster Analysis. You can specify which document types to process: • Documents • Presentations • Spreadsheets • Email You can also specify the similarity threshold, which determines the level of similarity required for documents to be considered related or near duplicates.
	Generate System Information	Extracts data and populates the *System Information* tab. See Viewing System Information on page 403.
Miscellaneous tab		
File Type Identification	*File Signature Analysis*: Analyzes files to indicate whether their headers or signatures match their extensions. Before version 5.1, when performing additional analysis, if you selected certain processing options, such as *Flag Bad Extensions*, *dtSearch Text Index*, *Data Carve*, *OCR*, *Explicit Image Detection*, or *Decrypt Credant Files*, the *File Signature Analysis* option was automatically selected and the option was disabled so that you could not un-select it. Stating in version 5.1, if you select one of those options, the *File Signature Analysis* option is still automatically selected, but the option is not disabled and you can manually un-select it. Disable this option with care. This does not apply to the initial processing options.	
Carving	Carves data immediately after pre-processing. Click **Carving Options**, then select the file types to carve. Uses file signatures to identify deleted files contained in the evidence. All available file types are selected by default. For more information on Data Carving, see Data Carving (page 91). Selecting this will also enable the *Expand Compound Files* option.	
Miscellany		
	Expand Compound Files (Email, OLE, ZIP, etc.):	Expands and indexes files that contain other files. *Include Deleted Files*. Checked by default. Uncheck to exclude deleted files from the case. See Expanding Compound Files on page 85.
	Create Thumbnails for Graphics:	Generates thumbnails for graphic files found in the evidence. Thumbnails are always .JPG format, regardless of the original graphic format. See Examining Graphics on page 315.

Additional Analysis Options (Continued)

Field Item	Description	
	Create Thumbnails for Videos	Creates thumbnails for all videos in a case. You can also set the frequency for which video thumbnails are created, either by a percent (1 thumbnail every “n”% of the video) or by interval (1 thumbnail every “n” seconds. See Examining Videos on page 326.
	Generate Common Video File	When you process the evidence in your case, you can choose to create a common video type for videos in your case. These common video types are not the actual video files from the evidence, but a copied conversion of the media that is generated and saved as an MP4 file that can be previewed on the video tab. See Examining Videos on page 326.
	Flag Bad Extensions:	Flags files that have extensions that do not match the file headers.
	HTML File Listing:	Generate a list of files contained in the case, in HTML format.
	CSV File Listing:	Generate a list of files contained in the case, in CSV format. This list can be used in any CSV supported spreadsheet application.
	Don’t Expand Embedded Graphics.	This option lets you not process embedded graphics from email items. The default behavior has not changed. This option only applies if you select it in the processing options.
	Process Internet Browser History for Visualization	Processes internet browser history files so that you can see them in the detailed visualization timeline. See Visualizing Browser History Data on page 294.

Hashing

When the MD5 Hash option is chosen for evidence processing, the MD5 hash value for every file item discovered within the evidence is computed. The same is true for SHA-1 Hash and SHA-256 options. In general, a hash value can be used (in most situations) to uniquely identify a digital file - much like a finger print can uniquely identify the person to whom it belongs.

Several specific purposes are served by enabling hashing during processing. First and foremost, when the MD5 Hash and/or SHA-1 Hash options are chosen along with the KFF option, each file item's MD5 (and/or SHA-1) value can be found within the KFF Library. The KFF Library does not contain any SHA-256 values. All of the file items within the evidence that have been encountered and reliably cataloged by other investigators or US Federal Government archivists can be identified. This feature lets you find the "known" files within the evidence, which brings some intriguing advantages to the investigator.

These are described in Using the Known File Filter (KFF) (page 264).

Data Carving

Data carving is the process of locating files and objects that have been deleted or that are embedded in other files.

You can recover and add embedded items and deleted files that contain information that may be helpful in forensic investigations.

The data carving feature allows the recovery of previously deleted files located in unallocated space. Users can also carve directory entries to find information about data or metadata.

Note: You can create custom carvers. In addition, you can manually carve for any file type for which you have the correct header/footer/file length information, then save that file and add it to the case. In addition, you can carve any data from any file, and save the selected data as a separate file and add it to the case.

See also Custom Carvers (page 93).

To recover embedded or deleted files, the case evidence is searched for specific file headers. Using the data from a file header for a recognized file type the length of that file is determined, or the file footer is found, and "carves" the associated data, then saves it as a distinct file. A child object is created with a name reflecting the type of object carved and its offset into the parent object's data stream. Embedded or deleted items can be found as long as the file header still exists.

Data carving can be done when adding evidence to a case, or by clicking **Evidence > Additional Analysis > Data Carve** from within a case.

Recognized File Types for Data Carving

• AOL Bag Files	• LNK Files
• BMP Files	• OLE Archive Files (Office Documents)
• EMF Files	• PDF Files
• EML Files	• PNG Files
• GIF Files	• TIFF Files

Recognized File Types for Data Carving (Continued)

• HTML Files	• Zip Files
• JPEG Files	

You can set additional options to refine the data carving process for the selected file types.

Data Carving Files When Processing a New Case

Data Carving can be done during initial case creation by setting preprocessing options, or later, as an Additional Analysis task.

Viewing the Status and Progress of Data Processing and Analysis

The *Data Processing Status* screen lets you view the status of any processing, analysis, or searching that is being done on evidence in a case. This screen is also called the *Progress Window.*

To view the status and progress of data processing and analysis

1. In the *Examiner*, click **View > Progress Window** to open the *Data Processing Status* screen.
   Processing is categorized according to the following job types:
   - Add Evidence
   - Additional Analysis
   - Live Search
   - Other
2. Click on a job type in the left pane, to view aggregate progress statistics for all of the items in a job type.
3. Click the expand icon to the left of a job type and then select an individual job or task to view the status of jobs and tasks.
   Details about each task in a job are displayed in the right hand pane under **Messages**.
   You can also view the following status information about job processing:

Information	Description
Overall	The percentage complete as each task progresses.
Discovered	The number of items that have been discovered.
Processed	The number of items that have been processed. If you compare the numbers in the *Data Processing Status* screen with the numbers shown in **Overview tab > Case Overview > File Category**, for example, you may notice that the numbers are not the same. If there is a difference, the numbers in the case are accurate; the numbers in the *Data Processing* screen on the progress bar items are not.
Indexed	The number of items that have been indexed.
Process State	The current status of a job's processing. When the job is complete, this field displays Finished, and the Message box in the right pane also displays Job Finished.
Name	The file name of the evidence item that is processing in a task.
Path	The path to where the evidence item is stored.
Process Manager	The Process Manager computer is listed by its name or by its IP Address. If your Evidence Processing Engine runs on the same computer as the *Examiner* and the database, then "localhost" is the default Process Manager. If you are using Distributed Processing, the Process Manager or the Remote Processing computer is listed.

4. You can select from the following options:
   - **Job Folder** lets you open the location where the JobInformation.log for this job is stored. You can view detailed information about the processing tasks and any errors or failures in the JobInformation.log file.
   - **Remove when finished** lets you remove a task or job from the job list when it has completed processing.
   - **Pause** lets you pause the current evidence processing task and adds an entry in the Messages box listing the date and time it was paused.
   - **Resume** lets you resume the current processing task after having paused it and adds an entry in the Messages box listing the date and time processing was resumed. This option only appears after the **Pause** option has been enabled.
   - **Cancel** lets you stop the current task from running.
5. Click **Close** to close the display but not cancel any current tasks.

Viewing Processed Items

It is not necessary to wait for the program to finish processing the case to begin viewing data. The metadata—the information about the evidence—can be viewed in several modes before the evidence image has completed processing.

Important: Do not attempt to do any search prior to processing completion. You can view processed items from the tabbed views, but searching during indexing may corrupt the index and render the case useless.

Chapter 9

Working with Live Evidence

You can acquire live evidence from local and remote network computers. Adding and using both local and remote live evidence is covered in this chapter.

See also About Acquiring Digital Evidence (page 26) for details on the ways that evidence can be acquired, and precautions to take before acquiring evidence.

This chapter includes the following topics

- About Live Evidence (page 144)
- Adding Local Live Evidence (page 145)
- Methods of Adding Remote Live Evidence (page 146)
- Requirements for Adding Remote Live Evidence (page 146)
- Adding Evidence with the Temporary Agent (page 147)
- Adding Data with the Enterprise Agent (page 149)

About Live Evidence

Data that you gather and process from an active data source is called live evidence. You can gather this data from either local or remote sources.

Types of Remote Data to Acquire

Data Types found in RAM	Memory Data	Drive Data
• Process Info • DLL Info • Sockets • Driver List • Open Handles • Processors • System Descriptor Tables • Devices	• RAM • Memory Search	• Physical Drives • Logical Drives • Mounted Devices

Some live evidence like processes and services information may fluctuate and change frequently. This evidence is called volatile data. Volatile data is different than memory data and does not contain the same information as a

Memory Data (RAM) acquisition. A RAM acquisition downloads all the RAM data into a memory dump, and then it is read and processed when you add it to a case.

Drive data includes physical drives and devices, logical drives and devices, and mounted devices on a remote computer.

Administrative rights and permissions are required on the remote computer to collect remote live evidence. See Requirements for Adding Remote Live Evidence on page 146.

Types of Live Evidence

Live evidence is data that you gather and process from an active data source. It is important to understand any implications of acquiring data live. See About Acquiring Digital Evidence on page 26.

You can acquire and investigate the following types of live evidence:

- Local live evidence.

  An example of local live evidence is an original drive or other electronic data source that is attached to the investigation computer. It can also be data acquired from a device on a remote computer while the device is mounted to the system as Read/Write.

  See Adding Local Live Evidence on page 145.

- Remote live evidence.

  You can acquire data directly from computers on your network. This data is called remote live evidence. The process of adding the data into a case is called remote data acquisition.

Adding Local Live Evidence

You can add live evidence and then create a static image of that data. You can also add the data without creating an image, but realize that as the files are read, the operating system makes changes to the file statuses, the Read date and time stamps, and the Accessed time and date stamps. You can add the entire contents of a folder or a single file from a device that is attached to the *Examiner* machine.

To add live evidence to a case

1. In *Examiner*, click **Evidence > Add/Remove.**
2. In the *Manage Evidence* dialog box, click **Add**.
3. Do one of the following:
   - Click *Contents of a Directory*, then click **OK**. Browse to and select the directory. Read the warning. To continue click **Yes**.
   - Click *Individual Files*, then click **OK**. Browse to the location, select one or more files. You can use Shift-Click or use Ctrl-Click to select multiple files. Read the warning. To continue click **Yes**.
   - Click *Physical Drive*, then click **OK**. Read the warning. To continue, click **Yes**. Select a drive. The drives are listed in UNC format and are pre-pended with the string: PHYSICALDRIVE. Click **OK**.
   - Click *Logical Drive*, then click **OK**. Read the warning. To continue, click **Yes**. Select a drive. The drives are listed by drive letter. Click **OK**.
4. A job is created and the *Data Processing Status window* opens. Live Evidence Jobs are displayed under *Other Jobs*.
5. Click **Close**.

Methods of Adding Remote Live Evidence

There are two agent applications that you can install on networked computers to add remote live evidence.

The following agents are included:

- Temporary Agent.

  The Temporary Agent is an application for short-term use on client computers to access and acquire specific remote live evidence. It is set to expire after a period of inactivity and then it automatically uninstalls itself.

- Enterprise Agent.

  The Enterprise Agent is a persistent agent application for client computers that lets you remotely perform administrative tasks such as memory searches, memory dumps, memory analysis, remote device mounting and device acquisition.

Requirements for Adding Remote Live Evidence

To use *Add Remote Data* the following requirements must be met:

- Your user account must have the Application Administrator or the Case Administrator role. Case Reviewers cannot access the *Add Remote Evidence* dialog.
- Your Windows user account must have local administrator rights on the computer from which you want to acquire the data.
- An Agent must be installed on the target remote computer.

> **Note:** On Windows Vista, Windows 7, and Windows Server 2008 systems, the application must be run as an administrator in order to push agents to remote computers. To run as administrator, you can right-click on the desktop icon and click, run as administrator.

Simple File Sharing must be disabled on Windows XP targets. The default setting is enabled.

Important: The following are not supported on client computers running Windows 8 and 10:

- Memory Analysis
- Memory Acquisition
- Import Memory Dump
- Volatile Memory

Adding Evidence with the Temporary Agent

The Temporary Agent can acquire forensic images of the physical and logical drives, acquire non-proprietary images of memory, and forensically mount physical devices or logical volumes to the *Examiner* computer. You can remotely mount up to three devices simultaneously.

When you deploy the Temporary Agent, it automatically creates and uses a temporary certificate for secure communications. This certificate automatically expires and is only valid for a limited scope.

Pushing the Temporary Agent

You can push the Temporary Agent to a remote computer to acquire data. The temporary agent remains active until it has not had any activity for a short period of time. After the period of time is over, the Temporary Agent automatically uninstalls itself. You can also manually disconnect the agent from the *Tools* menu in *Examiner*.

Certain requirements must be met in order to deploy the temporary agent. See Requirements for Adding Remote Live Evidence on page 146.

To push the Temporary Agent

1. In the *Examiner*, click **Evidence > Add Remote Data**.
2. Enter either the IP Address or the DNS hostname of the target computer.
3. Make sure that a *Remote Port* is designated to use. The default port is 3999.
4. Choose **Install a Temporary Agent**.
5. Click **OK**.

> **Note:** In Windows, if the user has defined a TEMP\TMP path different from the system default TEMP\TMP path, the agent will push successfully to the machine, but will not run properly.
>
> To workaround, make sure that the TEMP / TMP environment variables are set to:
> *%USERPROFILE%\AppData\Local\Temp*

6. Enter the credentials of a user who is a member of the local administrators group on the target computer.

> **Note:** The authentication domain is required for both domain accounts and local accounts. If using a local account, enter the IP address or the DNS hostname of a local administrator account.

7. Click **Add** to add the set of credentials to the list.
8. Click **OK**.
9. In the *Remote Data* dialog, select from the following options to acquire and click **OK**.
   - *Image Drives*: Lets you create an image of a drive or device on the remote system. You can store the image on the remote computer or on the *Examiner* computer. You can also automatically add the image into a case.
   - *Acquire RAM*: Lets you acquire the data currently held in memory on the target machine. You can also capture and automatically import a memory dump, or save the memory dump to a location. See also Importing Memory Dumps (page 157).
   - *Mount Device*: lets you mount a remote drive or device and view it in Windows Explorer as if it were attached to your drive. It can be a CD or DVD, a USB storage device, or a drive or partition. See also Unmounting an Agent Drive or Device (page 157).

Note: The *Preview Information Only* option is not available for the Temporary Agent.

The job begins and the *Data Processing Status* window opens. *Acquire Remote Data* jobs are displayed under *Other Jobs*. Click **Close** to close the *Data Processing Status* window.

Manually Deploying the Temporary Agent

You can manually install the agent and the required certificate key.

Requirements for Manually Deploying the Temporary Agent

- Either a self-signed certificate, or a CA-signed certificate to run the manual deployment from a thumb drive.
- Administrator privileges on the target computer.
- Network connectivity to the target computer.

To manually deploy the Temporary Agent

1. Copy the appropriate Agent.EXE (32-bit, or 64-bit) from
   C:\Program Files\AccessData\Forensic Toolkit\<version>\bin\Agent\x32 (or x64)
   to a thumb drive or a shared network resource that is available to both the host and the target machines.
2. Copy the public key certificate file to the same thumb drive or a shared network resource. If you used the *Examiner* to create a certificate, the file is stored by default at:
   C:\Program Files\AccessData\Forensic Toolkit\<version>\bin\
3. Create a new folder on the target machine.
4. Copy the CRT and agent files from the thumb drive or shared resource to the new folder.
5. Open a command line and navigate to the path of the Agent2 folder.
6. Run one of the following command lines, depending on if the agent is 32-bit or 64-bit.
   ftkagent.EXE -cert [certname.crt] -port [portnumber]
   ftkagentx64.EXE -cert [certname.crt] -port [portnumber]
7. Depending on which agent file you deployed, you will see either FTKAgent.EXE or FTKAgentx64.EXE in the Task Manager. *Do not* close the command line, or the agent uninstalls.

Adding Data with the Enterprise Agent

The Enterprise Agent lets you acquire data from remote systems in your network. You can map to a remote drive and preview the contents before adding it to the case.

Methods of Deploying the Enterprise Agent

You can use the following methods to deploy the Enterprise Agent to remote computers:

- *Push agent*: You can use *Examiner* to deploy the Enterprise Agent from the server to remote computers.
- *Manual installation*: You can manually install the agent executable and the required public certificate key on the target machine.
- *Network deployment*: The Enterprise Agent can be also deployed with other means. For example with Active Directory, or with third-party software management utilities.

Creating Self-signed Certificates for Agent Deployment

Communication between the Enterprise Agents and the *Examiner* computer are transmitted on a Secure Socket Layer (SSL) encrypted channel. The SSL certificates can be either self-signed within the *Examiner*, or signed by a Certificate Authority (CA).

You must have three types of communications certificates to use the Enterprise Agent. These include a private key, a corresponding public key, and trusted certificate that AccessData provides when you install.

Once you have the certificates, you must configure the communications settings before you can push the agent to remote computers.

For more information see Configuring Communication Settings for the Enterprise Agent Push (page 150)

You can use the *Examiner* to create self-signed certificates.

Creating Self-Signed Certificates with Certman

Certman is a utility, bundled with several AccessData products, that can be used to generate self-signed certificates. These certificates can be used with the Enterprise Agent and other AccessData products. The steps below will demonstrate how to use Certman.

Prerequisites:

- Copies of certman.exe, libeay32.dll, and boost_thread-vc100-mt-1_49.dll, all in the same folder (typically found in [Drive]:\Program Files\AccessData\Forensic Toolkit\[version]\bin\certman.exe)

To Create Self-Signed Certificates with Certman

1. Open a Command Prompt (as Administrator)
2. Navigate to the folder containing certman.exe

3. Run the following command to generate a self-signed public/private key pair:

   certman.exe -e -n <issuer> <certificate_name>

   Where <issuer> is the name of the local PC where Certman is being run (including domain, if applicable), and <certificate_name> is what you'd like to name the certificate.

   Certman will generate a P12 key package, KEY private key, and CRT public certificate in the same folder as certman.exe

   Example:

   If my PC were named "ADPC", on the "adlocal.com" domain, and I wanted my certificates to be named "MyCert", I'd run the following command:

   certman.exe -e -n ADPC.adlocal.com MyCert

   This would produce a key package named MyCert.p12, a private key named MyCert.key, and a public certificate named MyCert.crt.

Note: The resulting P12 key package will be unencrypted, allowing it to be imported into IIS (without a password).

Configuring Communication Settings for the Enterprise Agent Push

You must set up the Enterprise Agent communications settings before you can push the agent to target computers.

To use the Enterprise Agent, you must provide certificates for a public and private key.

For more information see Creating Self-signed Certificates for Agent Deployment (page 149).

To configure communications settings for the Enterprise Agent push

1. In the *Examiner*, click **Tools > Configure Agent Push**.
2. In the *Configure Agent Push* dialog, configure the following options:

Option	Description
Path to UNC share	The network path to the share formatted as a UNC. Do not include the server name portion of the path. For example, if the path is \\TARGETSYSTEM\SHARE\, then enter \SHARE\. It is recommended to use a path that is ubiquitous across all target systems. For example, the ADMIN$ share.
Local path to shared folder	The same directory specified in the *Path to UNC Share* field, but written in a local folder syntax. The agent requires a local path in order to execute its tasks.
Path to trusted modules certificate	This is an AccessData supplied certificate that is automatically added when you install. You should not normally need to modify this location.
Path to agent modules	This is the location on the *Examiner* computer where the agent modules files are stored. You should not normally need to modify this location.

Option	Description
Path to public key	The public key that is to be used by the agent. The public key can be either a CERT or a P7B. A P7B file is a container of certificates with a chain of public keys up to the Certificate Authority.
Path to private key	This is the location of the private key certificate. For example this can be PXCS12, PFX, PEM, P12, PEM.ADP12, or P12.ADP12. ADP12 is an AccessData protected and encrypted P12 certificate. The *Examiner* automatically creates and uses ADP12 private keys when you supply it with a PEM or P12 private key.
Agent port	By default the agent is configured to listen on port 3999. You can use this field to configure the agent to use a different port.

3. Click **OK**.

Pushing the Enterprise Agent

You can push the Enterprise Agent from the server to remote computers.

Before you can do this task, you must first configure your Enterprise Agent settings.

See Configuring Communication Settings for the Enterprise Agent Push on page 150.

To push the Enterprise Agent

1. In *the Examiner*, click **Tools > Push Agents**.
2. Do one of the following:
   - In the *Machines to install* field, enter an IP address, or a DNS hostname for target computer and click **Add**.
   - Click **Import** to add a list computers from a file.
3. Choose from the following options:

Option	Description
Uninstall Agent	Lets you uninstall the agent from a computer that already has it installed. See also Removing the Enterprise Agent (page 152)
Use custom agent name	Lets you rename the agent process. For example you can use the field to rename the process to something more descriptive, or less descriptive. You can change the following names: Service name Executable name

Option	Description
Update the agent if it is present	Checks if an existing agent is already installed and upgrades it to the most current version on your server.
Allow manual uninstall	Lets the user on the target computer remove the agent from the Windows Add or Remove programs window.

4. Click **OK**.

Removing the Enterprise Agent

You can use *Examiner* to remotely uninstall the Enterprise Agent from target computers.

To remove the Enterprise Agent

1. In the *Examiner*, click **Tools > Push Agents**.
2. Do one of the following:
   - In the *Machines to install* field, enter an IP address, or a DNS hostname of the target computer and click **Add**.
   - Click **Import** to add a list computers from a file.
3. Select *Uninstall Agent*.
4. Click **OK**.

Connecting to an Enterprise Agent

To connect to the Enterprise Agent

1. In *the Examiner*, Click **Evidence > Add Remote Data**.
2. Enter the IP Address of hostname or target machine where Agent is deployed.
3. Enter the port to connect to the agent. By default the agent uses port 3999.
4. Select **Use Existing Agent.**
5. Click **OK**.
6. Browse to the **Agent** folder and choose the certificate file and click **OK**.
7. Choose from the list of options the ones to use during this session.

Adding Remote Data with the Enterprise Agent

To add remote data, in the *Examiner*, click **Evidence > Add Remote Data**. Once the remote data is added to the case, you can view it in the *Volatile* tab.

The Enterprise Agent can add the following types of remote data:

- Volatile Data
- Memory Data
- Drive Data

- Mounted Device Data

You can make these selections each time you do an acquisition, or you can set defaults that are applied automatically. Default preferences still let you change your final selections before you submit the job.

You can dump processes and DLLs into a file. You can acquire and add RAM data immediately, or save it to a memory dump file to import later. Page files and swap files are also supported.

To add remote data with the Enterprise Agent

1. Connect to an Enterprise Agent. See Connecting to an Enterprise Agent on page 152.
2. In the *Add Remote Data* dialog, in the *Selection Information* pane, choose from the following remote data options to acquire:

Note: It is recommended to do *RAM* acquisitions separately from *Volatile Data* acquisitions. A volatile acquisition pulls may override the RAM acquisition settings, and prevent the proper acquisition of data such as the system descriptor tables.

Option	Description
Include Volatile Data	Lets you select to include from the following volatile data types: • *Process Info* - Shows details of all processes. For example the process name, time, and hash. • *Service Info* - Returns details about which services are available according to the operating system. For example this includes the status such as stopped and running, and the startup type such as manual and automatic. • *DLL Info* - Returns details about load-time specific DLLs for a process. This does not return run-time DLLs. • *Driver Info* - Returns the drivers on the target computer. • *User Info* - Returns details about the users that have a local account on the computer. This option also returns the shares that each user has mounted at the time of log-on. • *Open Handles* - Returns the open handles of a specific process. For example: registry, files, sockets, and other items that can be associated by a handle. • *Network Sockets* - Returns the open sockets for a process. • *Network Devices* - Returns devices from the target such as NICs, Gateways, and routing. • *Registry Info* - Lets you discover if specific keys are present. This opens the *Acquire Registry Keys* dialog where you can select from predefined options or create your own customer path to retrieve.
Include Memory Data	Lets you select from the following memory information: • *RAM* – lets you either run a memory analysis, or capture a memory dump. A memory analysis instructs the agent to analyze live memory and returns a volatile snapshot of it. A memory dump lets you capture the live memory into a file. You can specify a path to store the file or to automatically add and analyze the dump in your case. • *Memory Search* – Lets you search for items in memory such as specific processes, DLLs, text, or even Hexadecimal values.
Include Drive Data	Lets you capture or preview either a logical or physical view of the drive. Some drive configurations require viewing them from a logical perspective or from a physical perspective. For example, drives configured in software RAID array versus drives configured in a hardware RAID array. You can either create an image of the drive or a preview of the drive. The Image option creates a forensic image of the drives. You can automatically add it or you can store it in a location. The preview option adds the metadata of the drive as an evidence item. You can use this to quickly view the file system within the interface to determine if more action is required. • *Physical Drive Info* – This option includes the drives as they are determined by the BIOS. • *Logical Drive Info* - This option includes the drive information as it is determined by the operating System. See also Acquiring Drive Data (page 155)

Option	Description
Mount a Device	Lets you mount a disk or device onto the *Examiner* computer that represents the targeted disk of the remote computer.

3. In the *Acquisition Options* pane, choose from the following options:

Option	Description
Include hidden processes	When you select a process view, this option compares it with a memory analysis view. You can use this option to see differences between what the operating system reports running compared to what is reported as running in memory.
Include Injected DLLs	This option returns data to help you determine whether or not a DLL has been substituted during the run-time of a process.

4. In the *Resource Usage* pane, select the resource usage option that you want to use. For certain operations like memory capture and drive imaging, this setting restricts the amount of CPU usage on the target computer. For example, you can use this option to lower the CPU usage and avoid performance impacts to the target computer.
5. (Optional) Click *Preferences* to create a set of options to be automatically selected when you open the *Add Remote Data* dialog.
6. Click **OK**.

Note: Depending on the options that you select in the Selection Information pane, you may need to provide additional details. For example, *Registry Info* has a dialog that opens to define specific keys to check for.

7. The *Data Processing Status* screen opens and the Other Jobs group is open, showing progress on each of the tasks you have requested.

   You can close the *Data Processing Status* window at any time. Click **View > Progress Window** to check job processing status. When the status indicates that all data has been collected, click the **Evidence** tab to view acquired physical and logical drives or drive images. Click the **Volatile** tab in the Enterprise *Examiner* UI to view the Volatile information.

   For more information, see Using the Overview Tab (page 306) and see Using the Volatile Tab (page 412).

Acquiring Drive Data

When examining drive data, you can choose to acquire information for previewing only, or you can acquire a complete disk image. A separate job is created for each selected data source associated with the machine, but does not include memory. These jobs can be monitored in the **View > Progress Window > Data Processing Status > Other Jobs** list.

To include drive data in an acquisition

This task is accomplished as part of a procedure for adding remote data.

For more information, See Adding Remote Data with the Enterprise Agent on page 152.

1. *Drive Data* requires you to make drive selections. In the *Select Drives* pane, expand the drive list for that Agent machine and select a drive to view that drive's information in the Details pane.

   Click **OK**.

2. In the *Drive Data* group box, select the type of drive data to be examined.

   Preview Information Only: Provides a list of the files in the drives, not the actual files themselves.

   2a. Select *Include Slack* to detect fragments of files that have not been completely overwritten and/or *Recover Deleted Files* to recover deleted files that have not been overwritten.

   2b. **Complete Disc Image:** Creates an image of the drives. This process may take a long time and can impact the CPU usage of the remote computer.

   2c. Specify the *Disk Image Path* information relative to **This** (local) **machine** or **Remote source machine**.

   2d. Enter or browse to locate the **File Path** for the disk image.

   2e. If you chose **Remote source machine,** enter a user name and password for a location where you have permissions to write the image.

   2f. Mark **Add image to case when complete** to begin investigating the data as soon as the acquisition is complete. The evidence processor uses the default analysis options.

3. Click **OK** to start the acquisition.

Acquiring RAM Data

1. In the *Add Remote Data > Browse and Select Nodes* pane, select the Agent to acquire RAM data from.
2. In the *Selection Information* pane, click **Include Memory Data** if you want to acquire the RAM data and perform a memory search at the same time. If not, choose the option that suits your needs.
3. Make other selections for *Acquisition Options*, *Update Agent*, and *Resource Usage*, then click **OK**.
4. Do one of the following:
   - Choose either *Memory Analysis* to add the RAM data directly to the case you are working on.
   - Choose *Memory dump* to save the dump file to a destination folder and name of your choosing.
5. Click *OK*.

   If you chose *Memory Analysis*, the *Data Processing Status* dialog opens to display the memory acquisition jobs you requested. If you chose *Memory dump*, the *Memory Dump* dialog opens and you can continue to specify the options for the memory dump file.

   5a. *Specify a Memory Dump Location*. This can be a destination local to your *Examiner* machine, or on the remote Agent machine, but must be a location where you have full access permissions.

   5b. Choose a file type for the memory dump file. Options are RAW and AD1.

   5c. Select the box labeled *Add memory analysis to case* if you wish to do so.

   5d. Select the box labeled *Get memory page file* to make the memory page file available to the case.

   5e. Click **OK** to save settings and continue.

   The processing requests are added, the memory is acquired, and the search is performed as three separate jobs in the *Data Processing Status* window.

Importing Memory Dumps

The *Import Memory Dump* feature allows you to import memory dump files from this or other case files in to the current case.

Note: If importing a memory dump from a 64-bit target machine with more than 4 GB of RAM, it is strongly recommended that you use a 64-bit *Examiner*. The analysis may fail on a 32-bit *Examiner*.

To import a memory dump

1. In *the Examiner*, click **Evidence > Import Memory Dump**.
2. Select the system from the dropdown list. If the system is not listed, select the **<Add new Agent>** item from the list, and enter a hostname or an IP Address.
3. Click the **Browse** button to locate the memory dump file you want to add to your case and click **Open**.
4. Click **OK** to add the memory dump to your case.
5. The memory dump data appears in the Volatile tab in the *Examiner* window under the Agent name and acquisitions date and time. Each acquisition is displayed separately under its data and time stamp, grouped by Agent, Acquisition Time, or Operation Type.

   See also Using the Volatile Tab (page 412).

Unmounting an Agent Drive or Device

To Unmount a drive or device

1. Click **Tools > Unmount Agent Drive**.
2. In the *Unmount Agent Drive* dialog, do one of the following:
   - Select a drive to unmount.
   - Select *All Agents* to unmount all drives from all agents at the same time.
3. Click **OK**.

Chapter 10

Filtering Data to Locate Evidence

About Filtering

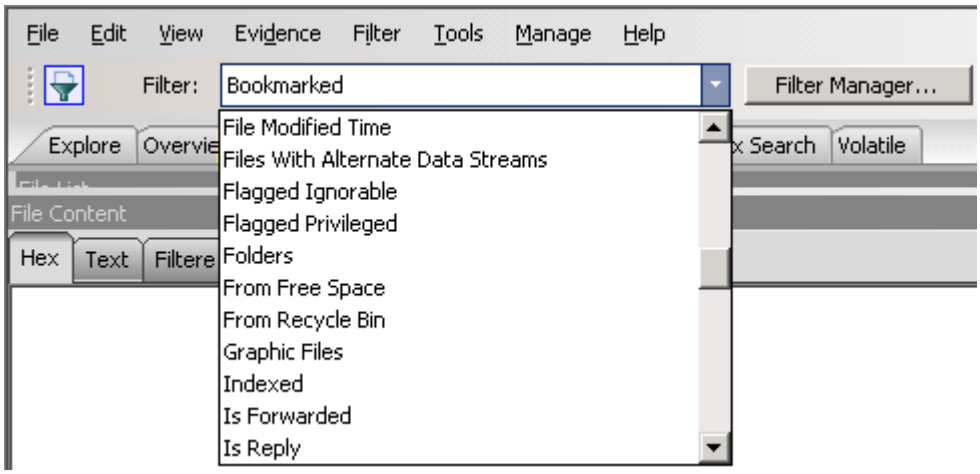
Filters let you leverage item attributes to locate specific data very quickly. They reduce the amount of time that you must examine data because they can narrow a large data set down to a very specific focus.

The *Examiner* includes a *Filter* toolbar, and a *Filter Manager* utility to help you work with filters. When you apply a filter it limits the files that are displayed in the *Examiner* match the criteria of the filter.

See also Types of Filters (page 159)

See also What You Can Do with Filters (page 159)

Examiner's Filter Dropdown Menu



Types of Filters

The *Examiner* includes several different types of filters to help you to locate and to exclude specific data.

Types of Filters

Filter Type	Description
Predefined Filters	Predefined filters are filters that AccessData has created. For example, there is a predefined filter called *Graphic Files* that limits the displayed data to graphics files only. You cannot delete or modify a predefined filter, however you can copy them to use as templates when you create your own custom filters. See also Types of Predefined Filters (page 170)
Global Filters	Global filters apply across the entire *Examiner* interface. For example, if you globally apply the filter *Checked Files*, only checked files are displayed, regardless of the tab, pane, or window that you are viewing. See also Using Global Filters (page 162)
Tab Filters	Tab filters apply only to a specific tab. For example if you apply the *Checked Files* filter as a tab filter specific to the *Overview* tab, when you switch to the *Explore* tab files that are not checked are still displayed. See also Using Tab Filters (page 162)
Custom Filters	Custom filters are filters that you create. For example if an AccessData predefined does not meet your exact needs, you can use the *Filter Manager* utility to create your own custom filter. See also Creating a Custom Filter (page 167)
Nested Filters	A nested filter is a filter that contains filters within it. Nested filters let you leverage several filters together to accomplish a specific goal. Nested filters prevent you from having to create a complicated custom filter each time you need to use multiple filters together. For example, a simple nested filter could include both *Graphic Files* and *KFF Alert Files* as filters. See also About Nested Filters (page 167)
Compound Filters	Compound filters are created in the *Filter Manager* utility. In the *Filter Manager* you can add many filters together. You choose to include and exclude a files that meet criteria. Compound filters let you apply boolean logic to your compound filter. See also Using Compound Filters (page 166)
Search Filters	Search filters are added to a live search or an index search. They limit a search to only display results that match the criteria contained within the search. You can use static search filters in conjunction with global filters to very quickly apply two levels of filtering to your search results. See also Using Filtering with Searches (page 165)

What You Can Do with Filters

You can use filters to quickly locate specific item types. You can also use filters to exclude data that you do not want displayed. For example, if you only want to see encrypted items, you can apply a filter to show you those. If

you do not want to see files that were created after a certain date, you can also use a filter to exclude those files from being displayed.

See also About Filtering (page 158)

What You Can Do with Filters

Task	Description
Apply filters globally	Using Global Filters (page 162)
Apply filters to specific tabs	Using Tab Filters (page 162)
Apply filters in categories	Using Filters with Category Containers (page 163)
Add filters to live searches	Adding a Search Filter to Live Searches (page 165)
Add filters to index searches	Adding a Search Filter to Index Searches (page 165)
Use filters when you create reports	Using Filters with Reports (page 163)
Create, copy, and customize your own filters	Creating a Custom Filter (page 167)
Share filters between cases	Sharing Custom Filters Between Cases (page 169)
Export filters	Exporting Filters (page 169)
Import filters	Importing Filters (page 169)

Understanding How Filters Work

Filters are composed of various components that are stored in your database.

Filter Component

Component		Description
Name	Filter names help you to locate a filter that you want to use.	
Description	Filter descriptions help you to understand what a filter is designed to accomplish.	
Rule	Filter rules instruct filters of the goal that you want to accomplish. Filters can have a single rule or filters can also have multiple rules. Filter rules are the logic that help you make your filters accomplish a specific task. Filter rules are comprised of the following components:	
	Property	Filter properties are the attributes that are associated with a data record. An example of a property is *File Type*.
	Operator	Filter operators are the decision that you want to run against a property. Each property has specific operators that are applicable to it. An example of an operator that applies to the property "*File Type*" is the operator "*Is Not*"
	Criteria	Filter criteria let you define the conditions of the operator. Each operator has specific criteria that are applicable to it. An example of criteria that applies to the property *Is Not* is the criteria *Word Template 2010*.

Note: When working with time-based filters, the case time zone is used for date and times offsets.

Viewing the Components of Filters

You can use the *Filter Manager* to see how any filter is constructed.

To view the definitions of a filter

1. In the *Examiner*, click **Filter Manager**.
2. In the *Filter Manager*, under the *Filters* list, select a filter.
3. Click **Define**. In the *Filter Definition* dialog, you can see the *Name*, *Description*, and any of the *Rules* that the filter uses.

Viewing Details about Attributes that Filters use

Each filter uses rules that leverage various attributes that are stored in the database. If you are unsure of what a particular filter attribute is, you can you can view descriptions about each of these attributes. To view these descriptions you must use the *Column Settings* utility.

To view details about attributes that are used by filters

1. In the *Examiner*, in the *File List* pane, click the **column settings** icon.
2. In the *Manage Column Settings* dialog, click **New**.

3. In the *Column Settings* dialog, under *Available Columns*, expand *All Features*.
4. Locate and select the attribute that you want to view details about.
5. Click **Add >>**.
6. In the *Selected Column* pane, the *Name*, *Short Name*, and *Description* are provided for the attribute.
7. When you are done viewing attribute descriptions, click **Cancel**.

Using Simple Filtering

You can accomplish the following simple tasks with filtering:

- Using Global Filters (page 162)
- Using Tab Filters (page 162)
- Using Filters with Category Containers (page 163)
- Using Filters with Category Containers (page 163)
- Using Filters with Reports (page 163)

Using Global Filters

You can apply filters globally across the files in the *Examiner*. Each filter limits which files are displayed in the *Examiner* pane according to the rules of the filter.

In the *Examiner*, you can keep a filter selected, and still turn it on and off.

See also Types of Filters (page 159)

To use a global filter

1. In the *Examiner*, in the upper-left menu bar, select the *Filter* drop-down menu.
2. In the *Filter* drop-down menu, locate the filter that you want to apply.
3. Click the filter.

   The results that are displayed in the *Examiner,* are limited to show only the files that are applicable to the filter that you select.

To turn global filters on and off

1. In the *Examiner*, do one of the following:

   - To turn a filter on or off, click the icon: that is next to the *Filter* drop-down menu. This leaves the filter that you have currently selected in place but activates or deactivates it.
   - If you no longer want to use any global filter, in the *Filter* drop-down menu, click **-unfiltered-**.

Using Tab Filters

You can create filters that are only applicable to a specific tab. These filters only apply to the tab that you create them in. If you have applied a tab filter its name is displayed at the bottom of the *Examiner* window.

See also Types of Filters (page 159)

To use a tab filter

1. In the *Examiner*, click **Filter > Tab Filter**.
2. In the *Tab Filter Selection* dialog, use the drop-down menu to select the filter that you want to apply.
3. Click **OK**.

If you have a tab filter applied, and no longer want to use it you can turn it off.

To remove a tab filter

1. In the *Examiner*, click **Filter > Tab Filter**.
2. In the *Tab Filter Selection* dialog, use the drop-down menu, select the empty field in the drop-down list. It is the first field in the drop-down menu.
3. Click **OK**.

How Global Filters and Tab Filters can work Together

Global filters and tab filters can be used together to further narrow down the data set that you are viewing. Using Global filters and Tab filters together is a quick way of apply two levels of filtering without creating or defining either a nested filter or a compound filter. For example, you can apply a global filter across all items in the case, and then create a specific tab filter to again further refine the data set to meet a criteria.

See also Using Global Filters (page 162)

See also Using Tab Filters (page 162)

Using Filters with Category Containers

The *Examiner* includes a tab called the *Overview* tab. The *Overview* tab groups items into categories. There are several different categories such as Documents, Executable files, Folders, and Graphics. You can use the *Overview* tab to first select a category, and then also apply a filter.

See also What You Can Do with Filters (page 159)

To use filters with category containers

1. In the *Examiner*, click the *Overview* tab.
2. In the *Case Overview* pane, locate and then click the category that you want to focus on.
   For example you could select, *File Category* > *Documents*. The *File List* pane would only display document files.
3. In the Filter drop-down select a filter that you want to apply.
   For example, you could select the filter *Encrypted Items*. The *File List* pane would then display only document files that are also encrypted.

Using Filters with Reports

You can apply filters when you create your reports.

See also What You Can Do with Filters (page 159)

To use filters with reports

1. In the *Examiner*, click **File > Report**.
2. In the *Report Options* dialog, select one of the following options:
   - *Bookmarks*
   - *Graphics*
   - *File Paths*
   - *File Properties*
3. In the upper portion of the *Report Options* dialog, click the *Filter* drop-down menu and select the filter that you want to apply.

   You can apply specific filter for each of the report options.
4. After you have finished defining the report, click **OK.**

Viewing the Filters that you have Applied

If you see results in the *File List* pane that don't match what you expect to see, it may because you inadvertently have filters applied that you didn't expect.

Check the following:

- To see if you have a global filter applied, in the upper-left portion of the Examiner, check the Filter field to see if a filter is applied. You can also check the filter icon to see if perhaps the filter is turned on or off.

- To see if you have a tab filter applied, in the lower bar of the Examiner, check to see if a tab filter is applied.

Using Filtering with Searches

You can apply global filters to modify the search results window. When you apply a global filter to a search, the search results window is modified to match the criteria of the global filter. Using global filters with searches lets you filter against a single search, without having to create a special search criteria for each filter type.

You can add search specific filters to a live search or to an index search. They limit a search to only display results that match the criteria contained within the search. When you add a search specific filter to a search, the search results window continues to limit the search results to apply to the filter.

You can use search filters in conjunction with global filters to very quickly apply two levels of filtering to your search results.

See Adding a Search Filter to Live Searches (page 165)

See Adding a Search Filter to Index Searches (page 165)

Adding a Search Filter to Live Searches

You can define a live search query, and add filter to limit the search results to meet your criteria.

See also What You Can Do with Filters (page 159)

To use a filter with a Live Search

1. In the *Examiner*, click the **Live Search** tab.
2. Use the tools in the *Live Search* tab to create and define your search query.
   Searching Evidence with Live Search (page 383)
3. In the *Search Filter* drop-down menu, select the filter that you want to apply to the search. The *Search Filter* drop-down menu is located in lower portion of the search pane. This operation limits the search results to only files that both meet the criteria of your search and the criteria of the filter.
4. In the lower-right portion of the search window, click **Search**.
   The search query is displayed in the *Live Search Results* pane.

Adding a Search Filter to Index Searches

You can define an index search query, and add filters to limit the search results to meet your criteria.If you have applied a filter, the filter's name is displayed in the *Search Results* pane.

See also What You Can Do with Filters (page 159)

To use a filter with an Index Search

1. In the *Examiner*, click the **Index Search** tab.
2. Use the tools in the *Index Search* tab to create and define your search query.
   Searching Evidence with Index Search (page 394)
3. Click **Search Now**.
4. In the *Indexed Search Filter* Option dialog, select **Apply filter**.
5. In the filter drop-down menu, select the filter that you want to use.

6. Click **OK**.

   The search query is displayed in the *Index Search Results* pane. If you have added a filter to the search, the search displays the follow string: *dtSearch® Indexed Search {Prefilter:(The Filter's Name) Query:(The Search's Syntax)*.

Using Compound Filters

Filters can be combined to more easily locate data. You can select and apply multiple filters at the same time. Such filters are called compound filters. The *Filter Manager* dialog provides a display of your compound filter to help you to visualize the resulting *Include* filter, or *Exclude* filter. You can choose **AND/OR** options to make your compound filters more effective.

Compound filters are not saved. They are only combined and applied as needed. As they are applied, the *File List* pane automatically displays the results of the applied filter. The filter remains applied until it is changed.

See also Applying Compound Filters (page 166)

Applying Compound Filters

Compound filters are applied in the Filter Manager.

See also Using Compound Filters (page 166)

To apply a compound filter

1. On the *Filter* toolbar, click **Filter Manager.**
2. Select a filter from the list of predefined filters to use as a template.
3. Choose from the following as needed:
   - Click the >> button, or drag and drop into the Include or Exclude box.
   - Click the << button to remove an individual item from either the Include or Exclude box.
   - Click **Clear** in either the Include or Exclude box to clear all items from that box and start over.
4. Click **Apply** at the bottom of the dialog. The results are displayed in the *File List* pane.

Using Custom Filters

You can create your own customized filters to meet your exact needs.

To save you the time and effort of creating filters, AccessData has created many predefined filters that you can leverage to accomplish the majority of your filtering tasks.

For more information see Types of Predefined Filters (page 170)

Before you create a new filter, you may be able to save time by copying a preexisting filter and modifying it to meet your specific criteria.

See also Copying Filters (page 168)

About Nested Filters

You can use the *Filter Manager* to create nested filters. A nested filter is a filter that contains multiple filters within it. You can add rules to a filter that check against other filters.

See also Types of Filters (page 159)

For example, the following illustrates the logic of a nested filter:

An Example of Rules for a Nested Filter

Filter	Matches	Graphics Files
Filter	Does Not Match	Flagged Ignorable
Filter	Does Not Match	KFF Ignore Files

Creating a Custom Filter

You can create your own custom filters. Filters are created from either the *Filter Definition* dialog or the *Filter Manager*.

To create a custom filter

1. In the *Examiner*, click **Filter > New**.
2. In the *Filter Definition* dialog, enter *Name* for the filter.
3. Enter a *Description* that explains what the filter does.
4. In the *Rules* section do the following to create a rule:
   - 4a. Select a *Property* from the drop-down menu.
   - 4b. Select an *Operator* from the drop-down menu.
   - 4c. Select a Criteria from the drop-down menu.
5. To add additional rules to the filter, click the + icon. To remove a rule, click the - icon.
6. If you want to turn a rule on, or turn a rule off, select the check box next to the rule.

Note: Select the checkbox at the top of the list to select all of the listed properties in the rules box at once.

7. In the lower portion of the *Filter Definition* dialog, do one of the following:
   - Select *Match Any* to force the filter to include or exclude files if they match any of the rules that you have defined in the filter.
   - Select *Match All* to force the filter to include or exclude files only if they match all of the rules that you have defined in the filter.
8. After you define the filter, click **Live Preview** to test that the filter is working as you expect. When you click *Live Preview* the contents in the *File List* pane adjusts to match the definition of the filter.
9. Click **Save**.
10. Click **Close**.

Copying Filters

You can copy any existing filter to use as a basis to create a new filter.

See also Types of Predefined Filters (page 170)

To copy a filter

1. In the *Examiner*, click **Filter Manager**.
2. In the *Filter Manager*, under the *Filters* list, select a filter.
3. In the lower portion of the *Filter Manager*, click the icon: **Create a copy of the selected filter**.
4. In the *Filter Definition* dialog, modify the filter according to your requirements.
5. Click **Save**.

Editing a Custom Filter

You can edit your own custom filters. You can edit the description and rules of a custom filter.

You cannot rename a custom filter. However, you can copy a filter, give the copy a new name, and then delete the original filter, if desired.

To edit a custom filter

1. In the *Examiner*, click **Manage > Filters > Manage Filters**.
2. In the *Manage Filters* dialog, select the filter that you want to edit.
3. Click **Edit**.
4. After editing the filter, click **Save.**

Sharing, Importing, and Exporting Filters

You can share filters between cases. You can import filters that have been created from other systems. You can also export custom filters that you have created to use in other systems.

See the following:

- Sharing Custom Filters Between Cases (page 169)
- Importing Filters (page 169)
- Exporting Filters (page 169)

Sharing Custom Filters Between Cases

After you create a custom filter for a case, you can share that filter to make it available to other cases. You can also copy filters from other cases to use in your case.

To share a filter with other cases

1. In the *Examiner*, click **Manage > Filters > Manage Filters**.
2. In the *Manage Filters* dialog, select the custom filter that you want to share with other cases.
3. Click **Copy to Shared**.
4. Click **Close**.

To copy a Shared filter into your Case

1. In the *Examiner*, click **Manage > Filters > Manager Shared Filters**.
2. In the *Manage Shared Filters* dialog, select the custom filter that you want to copy to your case.
3. Click **Copy to Case**.
4. Click **Close**.

Importing Filters

You can import filters that have been saved as XML files into your system.

See also Exporting Filters (page 169)

To import filters

1. In the *Examiner*, click **Filter Manager**.
2. In the *Filter Manager* dialog, click the **Import a filter from a xml file** icon.
3. In the *Open* dialog, browse to the location where the filter XML file is stored. Select the filter and click **Open**.
4. In the *Filter Import* dialog, click **OK**.

Exporting Filters

You can export filters into XML files to use in other systems.

See also Importing Filters (page 169)

To export filters

1. In the *Examiner*, click **Filter Manager**.
2. In the *Filter Manager* dialog, select the filter that you want to export.
3. Click the **Export selected filter to a xml file** icon.
4. In the *Save As* dialog, browse to the destination location where you want to save the exported filter file
5. Click **Save**.
6. In the *Export Filter* dialog, click **OK**.

Types of Predefined Filters

The *Examiner* includes several predefined filters that you can use for common filtering tasks. If these filters do not quite meet the criteria that you require, you can create a copy of these to create your own custom filters

See also Copying Filters (page 168)

Predefined Filters

Predefined Filter	Description
Actual Files	Shows the actual files, as opposed to All Files. All Files is the default and includes metadata, OLE files, and alternate data stream files.
Alternate Data Streams	Shows files with alternate data streams (additional data associated with a file object).
Archive Files	Shows only archive-type file items, such as ZIP and THUMBS.DB.
Bad Extension Files	Shows only the files with extensions that don't match the file header.
Bookmarked	Shows only the items that are contained in a bookmark.
Carved Files	Shows only the items that have been carved.
Cerberus Score	Shows only the items that have a Cerberus Score
Cerberus Static Analysis	Shows only the items that have had Cerberus Static Analysis run against them.
Checked Files	Shows only the items that you have selected with a check mark.
Decrypted Files	Shows only the items that have been decrypted by AccessData tools within the case. This indicates that AccessData decryption tools have had control of this file and its decryption since it was added to the case in its original encrypted form.
Deleted Files	Shows only those items that have the deleted status.
Duplicate Files	Shows only files that have duplicates in the case. This filter requires that you select the Flag Duplicate Files processing option.
eDiscovery Duplicates	A filter for eDiscovery duplicates.

Predefined Filters (Continued)

Predefined Filter	Description
eDiscovery Refinement	Includes files and folders that are not useful for most eDiscovery cases.
Email Attachments	Shows all email items that are not email messages.
Email Delivery Time	Allows definition of specific date/time range of email deliveries.
Email Files	Shows only those items that have the email status.
Email Files and Attachments	Shows all email items, both messages and attachments.
Encrypted Files	Shows only those items flagged as EFS files or other encrypted files.
Evidence Items	Shows all evidence items added to the case.
Excluded eDiscovery Refinement	Excludes files and folders that are not useful for most eDiscovery cases
Explicit Images Folder (High Score)	Shows folders with EID scores of 60 or higher using FST or ZFN (high) criteria.
Explicit Images Folder (Medium Score)	Shows folders with EID scores of 40 or higher using FST or ZFN (medium) criteria.
File Category	Allows user to set a filter by file category (is a member of). Relates to File Category tree under Overview tab.
File Created Time	Allows definition of specific date/time range of file creation.
File Extension	Allows filtering of files by a defined extension or set of extensions.
File Modified Time	Allows definition of specific date/time range of file modification.
Files with Alternate Data Streams	Shows files that contain Alternate Data Streams (additional data associated with a file system object).
Flagged Ignorable	Shows only those items you have identified as Ignorable.
Flagged Privileged	Shows only those items you have identified as Privileged.
Folders	Shows only folder items.
From Free Space	Shows only those items found in (carved from) free space.
From Recycle Bin	Shows only those items taken from the recycle bin.
Graphic Files	Shows only those items that have been identified as graphics.
Indexed	Shows items that have been indexed.
Is Forwarded	Shows any email item that has been forwarded.
Is Reply	Shows any email item that is a reply to another email.
KFF Alert Files	Shows all files with KFF Alert status that are in a case.
KFF Ignore Files	Shows all files with KFF Ignore status that are in a case.

Predefined Filters (Continued)

Predefined Filter	Description
Labeled Files	Shows files that have a Label assigned to them.
Microsoft Office Files	Shows Word, Access, PowerPoint, and Excel files.
Mobile Phone: Calendar	Shows calendar information acquired from a mobile phone.
Mobile Phone: Call History	Shows call information acquired from a mobile phone.
Mobile Phone: Messages	Shows message information acquired from a mobile phone
Mobile Phone: Phonebook	Shows contact information acquired from a mobile phone.
Mobile Phone Files	Shows files and data from mobile devices added to the case using AccessData Mobile Phone Examiner.
MS Office 2007/2010 Unimportant Subitems	Includes MS Office 2007/2010 Subfolders and Subfolders.
No Deleted	Shows all except deleted items.
No Duplicate	Shows only one instance of every item in the case.
No Email Related Files or Attachments	Shows files that are not Email related files.
No File Slack	Shows all except files found in (carved from) file slack.
No Files with Duplicates	Shows only files that have no duplicates in the case.
No KFF Ignore Files	Shows all items except KFF ignore files.
No KFF Ignore or OLE Subitems	Shows all items except KFF ignore files or OLE subitems.
No KFF Ignore or OLE Subitems or Duplicates	Shows all items except KFF ignore files, OLE subitems, or duplicate items.
No MS Office 2007/ 2010 Unimportant Subitems	Excludes unimportant files and folders contained in MS Office 2007/2010 OPC files (DOCX, XLSX PPTX etc)
No OLE Subitems	Shows all items except OLE subitems.
No Unimportant OLE Data Streams	Shows all items including OLE subitems, except that unimportant OLE data streams are not shown.
Not Flagged Ignorable	Shows all items except those you indicated Ignorable.
Not Flagged Privileged	Shows all items except those you flagged Privileged.
NSF Notes	Shows Emails, views, and other notes from Lotus Notes NSF databases.

Predefined Filters (Continued)

Predefined Filter	Description
OCR Extractions	Shows files that were extracted from graphics with OCR.
OCR Graphics	Graphic files that have been parsed by the OCR engine.
OLE Subitems	Shows only OLE archive items and archive contents.
Reclassified Files	Shows only those items whose classification you have changed.
Registry Files	Shows Windows 9x, NT, and NTFS registry files.
Subfilter for EID FST OR ZFN (high)	This is a subfilter that is used by the explicit images folder (high score) filter.
Subfilter for EID FST OR ZFN (medium)	This is a subfilter that is used by the explicit images folder (medium score) filter.
Thumbs.db Files	Shows Thumbs.db files.
Unchecked Files	Shows only those items that you have not checked.
Unimportant OLE Stream Categories	Shows only Unimportant OLE Stream Categories.
Unimportant OLE Streams	Shows only Unimportant OLE Streams.
User-decrypted Files	Shows only those items that you have decrypted and added to the case. Decrypted by User status is always applied to files added using the Add Decrypted Files feature. The *Examiner* cannot confirm validity, content, or origin of such files.
Video Conversion or Thumbnails	Shows only generated video thumbnails or common video files. See Examining Videos on page 335.
Video Thumbnails	Shows only generated video thumbnails. See Generating Thumbnails for Video Files on page 336.
Video Conversion	Shows only generated video common video files. See Creating Common Video Files on page 337.
Web Artifacts	Shows HTML, Index.dat, and empty Index.dat files.

Using the Persons of Interest Filter

Users can now scrape contact information from signatures in emails. Once a profile is created for the person of interest, investigators can use filters to search for data within the evidence. This allows investigators to pull contact information from disparate sets of evidence (laptop, mobile phone, email account) and connect information found in all items to one suspect. For example, investigators can pull contact information from an email signature, then filter based on the mobile phone number found there to connect phone calls, chats, or SMS communications to the same person of interest.

Visualization can be used once the People Finder filter has been applied for a visual picture of how the data relate.

Note: Persons of Interest Filters cannot be edited in the Filter Manager. They must be edited within the Persons of Interest windows.

To Process Data for Use with the Persons of Interest Filter:

1. In the *Evidence Processing* window, check the box next to the **Persons of Interest** option.
2. Click on the **Persons of Interest Options** box and select the **Scrape email signatures** option.
   If you would like to create your list of communication participants before the case is created, you may do so by clicking the **Persons of Interest** button within this window. But the data will not populate until after the evidence has been processed.
3. Click **Ok** and process the evidence.

Creating a List of Communication Participants

You must first add people to the Communication Participants list before you can create and run a filter.

To Add a Person Manually:

1. Open the *Persons of Interest* filter by clicking on the sillhouette icon in the menu bar. The *Communication Participants* window will open.
2. Click on the green plus icon at the bottom of the window. The *Add/Edit Person* window will open.
3. Type the desired name in the *Display Name* field.
4. Click **Ok**. The person will appear in the *Communication Participants* list.

To Edit a Person:

1. Open the *Persons of Interest* filter by clicking on the sillhouette icon in the menu bar. The *Communication Participants* window will open.
2. Click the **Edit** button.
3. Add or edit data as desired.
4. Click **Ok**.

To Delete a Person:

1. Select a name in the *Communication Participants* list.
2. Click on the red minus icon at the bottom of the window. A warning will appear asking if you are sure you want to delete the selected name.
3. Click **Yes**. The name will be deleted.

Creating a Rule within People Finder

To Create a Rule Manually within the Persons of Interest Filter:

1. Open the *Persons of Interest* filter by clicking on the sillhouette icon in the menu bar. The *Communication Participants* window will open.
2. Select or add a *Display Name* for your rule.
3. In the *Add/Edit Person* window, click the small plus icon in the left pane.
4. Select a *Type* in the dropdown menu.
5. Add an email or phone number to the *Data* field.
6. Click **Ok**.

Searching for Data within People Finder

To Add a Person Using Search:

1. Open the *Persons of Interest* filter by clicking on the sillhouette icon in the menu bar. The *Communication Participants* window will open.
2. Click on the green plus icon at the bottom of the window. The *Add/Edit Person* window will open.
3. Type the desired name in the *Find Person* field.
4. Click **Search**. The data will populate in the panel in grid form. These results will list everything that includes the search term in the email signature.
5. Select your desired email result. The data found in that email will be shown in list format underneath the results grid.
6. Select the data you want to include by checking the associated box and click the **Import** button.

   A filter rule (or rules) will be created for each selected item. It is also possible to add additional rules manually at this point.
7. Click **Ok** in the Filter Rule List pane. The person related to the selected data will be added to your *Communication Participants* list, along with all of their associated rules.

Creating a Communication Filter within People Finder

Once you have found the people, phone numbers, and email addresses you are searching for, you can create a filter to show all communications between specific persons of interest. Once created, the filter will appear in the *Filter* dropdown list and can be applied at any time.

To Create a Communication Filter:

1. Select one or more persons from the *Communication Participants* list.
   - Select one participant if you want to see all of their communications.
   - Select two or more participants to see how they communicate with each other.
2. Click **Create Filter**.
3. In the *Create Communication Filter* window, select the communication types to use in your filter.
4. Click **Ok**. A window will appear letting you know the filter was created, the name of the new filter, and asking if you would like to apply it to the current view.

5. Select **Yes** or **No**, then click **Close**.
   - If you select Yes, the *Examiner* will show all communications that fit the applied filter.
   - If you select No, you may apply the filter at any time using the *Filter* dropdown box in the *Menu Bar.*

Note: A yellow background will appear when a filter has been applied. This serves as a visual reminder that a filter is in effect.

To Edit a Person of Interest Communication Filter:

1. Open the *Persons of Interest* filter by clicking on the sillhouette icon in the menu bar. The *Communication Participants* window will open.
2. Select the same people that are included in the filter you wish to edit and click the **Edit** button.
3. Add or edit data as desired.
4. Click **Ok**.

Fields Searched when using Persons of Interest

Persons of Interest filters use an OR operator between the entries in accounts (phone numbers), and an AND operator between the people. The filter will only look for phone numbers specified for the listed people.

Email

The following fields are used to search for email addresses:

- To
- From
- CC
- BCC

Chapter 11

Working with Labels

Labels let you group files in the way that makes the most sense to you. Initially, there are no default labels. All are customized. Labels you create are saved locally and you have complete control over them within your case. However, labels can be created and shared to the database for use by all who have been granted access to do so.

This chapter includes the following topics

- What You Can Do With Labels (page 177)
- Creating a Label (page 178)
- Applying a Label (page 178)
- Managing Labels (page 179)
- Managing Label Groups (page 180)

What You Can Do With Labels

You can use labels to do the following

- Create bookmarks that contain only files with the labels that you specify.
- Apply labels according to common criteria, such as the following:
  - All Highlighted
  - All Checked
  - All Listed
  - Extend labels to associated (family) files; i.e., a label applied to a child file can also be easily applied to its parent. Thus, labels applied to a parent file can easily be applied to all of its children.
- Customize a column template to contain a labels column and sort on that column to view all of your case files according to the labels that are applied to them.
- Apply multiple labels to a single file.
- Multiple local labels can be selected and shared in one operation.
- Create group labels according to specific criteria.
- View labels in the *Overview* tab by the labels category and see all files with labels applied in the File List view.
- Share labels you create with the database to make them available for other cases, according to user permissions.
  - Shared labels do not affect existing local labels.

- Once a label is shared, it is managed by either the Application Administrator, or the Case Administrator.
- Shared labels can be pushed to cases, and can be saved (exported) and then added (imported) into other databases.
- Only Application Administrators can delete, import, or export Shared labels.
- Shared labels, once pushed to a case, become local, and are fully managed by the Case Administrator.
- Administrators can specify which shared labels are visible to which users.
- Case Administrators can change local labels and re-share them. If there is a duplicate name, you are given the choice to rename or cancel the operation.
- Case Administrators can update Shared labels from the database to their cases.
- Case Reviewers do not have permissions to Share local labels.

Creating a Label

You can use the File List view to create a new label.

To create a label

1. In the *File List* view, click **Create Labels**.
2. Click **Manage Local**. The *Manage Labels* dialog opens.
3. Click **New**. A text entry box opens on the first available line.
4. Enter a name for the label, and press enter. The label is saved with the default color; black.
5. Click **Change Color**. The *Color* dialog opens. You can use any color from the default palette, or click **Define Custom Colors** to create a unique color for this label. Use the cross-hairs and the slide to create the color you want, then click **Add to Custom Colors**, then select the custom color from the Custom colors palette.
6. Click **OK**. The *Manage Labels* dialog reopens. You can see your new label listed with the color you defined or selected.
7. Click **Close**.
8. Click **OK**.

Applying a Label

You can apply a label to a file or group of files to make them easy to locate.

To apply a label

1. In the *File List* view, highlight, check, or select the files you want to apply a label to.
2. Click the **Apply Label To** drop-down.
3. Choose whether to apply the label that you will select to **Highlighted**, **Checked**, or **Listed** files.
4. Click the **Apply This Label** drop-down and click on the label to apply to the selected files.
   The name of the label is displayed in that label's color.

Managing Labels

When you click the *Labels* button on the *File List* toolbar, and the *Labels* dialog opens, you see four buttons across the bottom.

The two buttons open separate dialogs that appear very much alike.

Aside from the different list of labels you may see, the only other difference you will see is the button that in *Manage (Local) Labels* says **Make Shared**, and in the *Manage Shared Labels* says **Copy to Case**.

Managing (Local) Labels and Managing Shared Labels Dialog Options

New	Click **New** to create another label.
Rename	Click **Rename** to change the name of any label you select.
Change Color	Click **Change Color** to select a different color for any label you select.
Delete	Click **Delete** to remove a label from the case. Deleting a label removes all instances of the label's application. The files remain, but the label itself is gone.
Import	Click **Import** to bring a label definition into your list from another source.
Export	Click **Export** to save a selected label definition for use in a different case.
Make Shared	Click **Make Shared** (from Manage (Local) labels) to Share a label definition to the database for others to use.
Copy to Case	Click **Copy to Case** (from Manage Shared labels) to copy a global label to a case that was created before that label was available.
Group	Click **Group** to create a labels Group that can be used locally or Shared to the database for others to use according to their permissions.

Managing Label Groups

Label groups are created by selecting labels that are shown in the *Label Groups* pane. Selection is done by a toggle method: click once to select, click again to deselect.

To create a new label Group

1. In the *Manage Label Groups* dialog, click **New**.
2. Provide a name for the new group.
3. Click **OK**.

Select any or all of the Groups to create new Groups. However, to add individual labels to groups, work in the Group Definition area, where there are two windows. On the left is *Labels Available to Add to Group*, and on the right is *Labels in Current Group*.

You must create a label before you can add it to the group. If the label you need is not listed in the Group Definition area, click **Close**. In the *Manage Labels* dialog, click **New** and create a label.

To add a label to a group

1. In the *Label Groups* window, select the group you want to add labels to.
2. Select a label in the left window and click the **>>** button to move it into the right window.
3. Repeat until the labels in the *Current Group* list are how you want.
4. Changes are saved as they are made. When you are finished adding labels to the group, click **Close**.

To remove a label from a Group

1. In the *Manage Label Groups* dialog, from the *Labels in Current Group* pane, highlight the label to be removed.
2. Click the **<<** button to move the label back to the *Labels Available to Add* pane.

Chapter 12

Decrypting Files

About Decrypting Files

If you have the correct credentials, you can decrypt many types of encrypted files in your cases.

Note: If you do not know the passwords for encrypted files, you can use tools to try to recover the password.

See Recovering Unknown Passwords of Encrypted Files on page 188.

When files are decrypted, the original encrypted files are maintained and a child object is created for the decrypted file. This results in two files that affects your file counts: one for the original file and one for the decrypted file.

The following tables list the methods you can use to decrypt files and the type of encrypted files that are supported

Decryption Methods

Encryption Type	Description
Automatic Decryption	AccessData Password Recovery Toolkit has been integrated so that you can decrypt several types of encrypted files. This integration is included and you do not need to have PRTK or DNA installed. For more information, see Decrypting Files Using the Automatic Decryption Processing Option (page 186)
Tools > Decrypt Files	From the Examiner interface, you can use the Decrypt Files option to decrypt one or more files. See Decrypting Files Using the Automatic Decryption Processing Option on page 186. See Decrypting EFS on page 190. See Decrypting Lotus Notes Files on page 193. See Decrypting S/MIME Files on page 193. See Decrypting Dropbox DBX Files on page 192.
Decrypting Credant files	You can configure Credant decryption either at the global application level or at the case level. See Decrypting Credant Files (Dell Data Protection | Encryption Server) (page 194)

Decryption Methods

Encryption Type	Description
When adding an encrypted image as evidence	When you add an image as evidence, if the image is encrypted with one of the supported types of encryption, it is automatically detected and you are prompted to enter the credentials.

The following table provides a list of the supported types that can be decrypted and the method used:

Files that can be Decrypted

Encryption Type	Description
• ABICoder • AdvancedFileLock • Apple DMG • AShampoo • BCArchive • BCTextEncoder • BestCrypt • CryptoForge • Cypherus • iOS backup files • Microsoft Office files • OpenOffice • PDF • PGP password file • RAR • StuffIt • TrueCrypt • WinZip adv.encryption • YAFFS (1 and 2) • ZIP • 7-Zip	Use the Automatic Decryption feature to decrypt these types of files. See Decrypting Files Using the Automatic Decryption Processing Option (page 186) If you do not know the passwords for these encrypted files, you can use tools to try to recover passwords. See Recovering Unknown Passwords of Encrypted Files on page 188. **Note:** When decrypting TrueCrypt files, it is decrypted as a filesystem image. You are not able to drill down into the image. As a workaround, export the decrypted file and re-add it as additional evidence.
Note: While BestCrypt BCArchive and BCTextEncoder are supported, BestCrypt encrypted volumes are not supported.	
• Windows Rights Management (RMS) for Microsoft Office files and Outlook email files	You can decrypt DRM files at the case level. See Decrypting Microsoft Office Digital Rights Management (DRM) Protected Files (page 191)
• Credant	You can configure Credant decryption either at the global application level or at the case level. See Decrypting Credant Files (Dell Data Protection | Encryption Server) (page 194)
• Dropbox • Lotus Notes (whole NSF) • Lotus Notes (notes/email) • Microsoft EFS, Office • S/MIME PKCS7	After initial evidence processing, you can use the Decrypt Files tool. See Decrypting Dropbox DBX Files on page 192. See Decrypting Other Encryption Types on page 190. See Decrypting Lotus Notes Files on page 193. See Decrypting S/MIME Files on page 193.

Files that can be Decrypted

Encryption Type	Description
• Bitlocker (Windows Vista, 7, 8) • Checkpoint/PointSec R73 7.4.5 • Checkpoint 7.6.150 with token challenge • McAfee Endpoint Encryption (formerly Safeboot) 5.x and 6.0 • Safeguard Easy 4.40.9 and Enterprise 5.40 and 5.50 • Symantec Endpoint Encryption (formerly Guardian Edge) 8.1.1, 9.1.6, 9.3.0, 9.4.1, 9.5.3, SEE version 8.0.1 • Symantec Drive Encryption (PGP WDE) 10.0 (only)	When you add an image as evidence, if the image is encrypted with one of these types of encryption, it is automatically detected and you are prompted to enter the credentials. See the following for more information: • Decrypting Bitlocker Partitions (page 196) • Decrypting Safeguard Utimaco Files (page 197) • Decrypting SafeBoot Files (page 199) • Decrypting Guardian Edge Files (page 199) • Decrypting an Image Encrypted With PGP® WDE (page 199)
• CheckPoint	

About the Encrypted File Passwords List

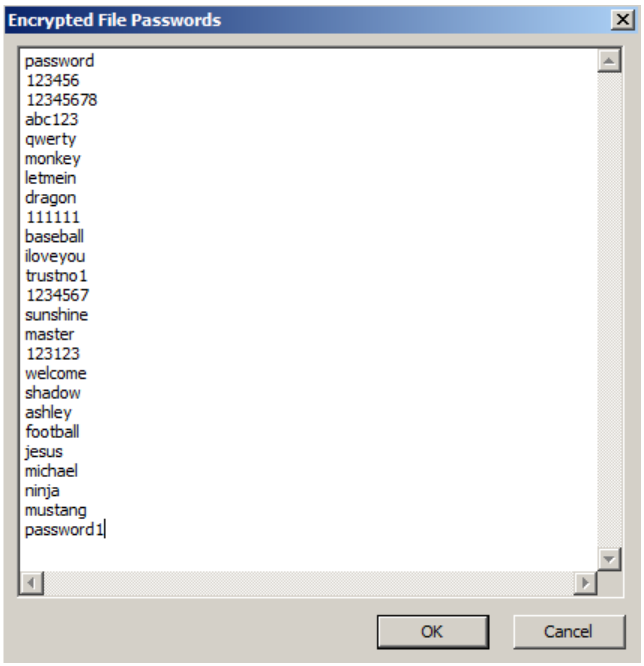
When you encrypt individual files, you create a list of passwords to use to try to decrypt the files. You configure a password list for each case.

When you enter passwords into the list, you can type them or paste them from a text file. Each password must be on its own line.

You can add passwords to the list at any time. The password list is saved with the case. The passwords are present any other time that you access the list in that case.

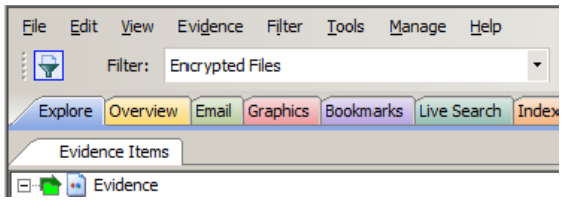
When compiling a list of passwords, you can use the following sources:

- Passwords that were recovered using AccessData PRTK or DNA
  See Recovering Unknown Passwords of Encrypted Files on page 188.
- Passwords that you have learned about as part of an investigation
- Lists of known commonly used passwords


Encrypted File Passwords
password
123456
12345678
abc123
qwerty
monkey
letmein
dragon
111111
baseball
iloveyou
trustno1
1234567
sunshine
master
123123
welcome
shadow
ashley
football
jesus
michael
ninja
mustang
password1
OK
Cancel

Identifying the Encrypted Files in a Case

After you have added evidence to a case, you can identify which files are encrypted. In the Examiner interface, you can use the Overview tab or apply the Encrypted Files filter.



To view the encrypted files in a case

1. Open the Examiner.
2. Do one of the following:
   - To use the Overview tab, do the following:

   2a. Click the **Overview** tab.

   2b. Expand **File Status**.

   2c. Click **Encrypted Files**

   - To use a filter, do the following:

   2a. Click the QuickPick icon for *Evidence* to view all or some of the of the evidence in the case.

   2b. Using the Filters drop-down menu, select **Encrypted Files**.

   In the *File List,* all decrypted files will be displayed.

After decrypting files, you can see which files have been decrypted.

See Recovering Unknown Passwords of Encrypted Files on page 188.

Note: In the File List, all decrypted files will be displayed in text. Several decryption key files are identified and categorized for ease of use. Find them in the *Overview* tab under **File Category > Other Encryption Files > Certificates**. Having these files identified and available makes it easier to quickly access files that may have been unavailable before.

Using PRTK/DNA Integration

Decrypting Files Using the Automatic Decryption Processing Option

You can decrypt many types of encrypted files using Automatic Decryption, which uses code from AccessData Password Recovery Toolkit (PRTK).

See About Decrypting Files on page 181.

To decrypt files, you supply a list of passwords. When the decrypted files are processed, those passwords are used to try to decrypt the files. If the passwords match, the files are decrypted.

You can configure and use this feature at any of the following times:

- As a processing option when doing one of the following:
  - Creating a case and configuring the default processing options for the case

    You can enable Automatic Decryption to be a default processing option for a case. As a default option, every time that you add evidence to the case, the default setting will be to try to decrypt files using the passwords that you provide. You can add passwords to the list at any time. This option is not enabled by default and will add time to the evidence processing.
  - Adding evidence to a case and configuring the refinement options for processing

    Any time that you add evidence to a case, you can configure the refinement options to enable file decryption using Automatic Description. Each time you enable decryption, you can modify that password list as needed.
  - After the evidence has been processed and using Additional Analysis

    Any time that you perform Additional Analysis, you can configure the refinement options to enable file decryption using Automatic Decryption. Each time you enable decryption, you can modify that password list as needed.
- After the evidence has been processed, from the Examiner interface using Tools > Decrypt files

The following encrypted file types cannot be decrypted using the Perform Automatic Decryption option during processing:

EFS, Lotus Notes (whole), Lotus Notes/emails, SMIME, and Credant

Instead, you must use the *Tools > Decrypt Files* option in the Examiner.

To configure Automatic Decryption as a processing option

1. Access the Processing Options for either a new case, new evidence or for performing Additional Analysis.
2. On the options page, check **Perform Automatic Decryption**.

   See Evidence Processing Options on page 82.
3. Click **Passwords**.
4. Enter the passwords that you want to use.

   See About the Encrypted File Passwords List on page 183.
5. Click **OK**.

To perform Automatic Decryption from the Decrypt Files page

1. In a case, click **Tools > Decrypt Files**.
2. In the *Decrypt Files* dialog, check **Perform Automatic Decryption**.
3. Click **Passwords**.

4. Enter the passwords that you want to use.
   See About the Encrypted File Passwords List on page 183.
5. Select **Attempt Blank Password** to decrypt files with no password, or whose password is blank.
6. Click **OK**.
7. Click **Decrypt**.
   A processing job is started to decrypt files.
   When using PRTK/DNA integration or recover a password, a dialog is displayed showing the progress of the recovery job. When a password has been recovered, the status in the dialog will turn green and it will display “A password has been recovered. Attempting to decrypt the file.”

   Note: You may briefly see a progress dialog appear. The dialog is not applicable to this data and will disappear quickly.
8. If needed, you can cancel the decryption process.

After decrypting files, you can see which files have been decrypted.

See Recovering Unknown Passwords of Encrypted Files on page 188.

Decrypting Files Using Right-Click Auto Decryption

The integration with PRTK/DNA includes an Auto Decrypt option. You can use a right-click option one an encrypted file in the File List and it will send the file to PRTK/DNA for password recovery. If the password is found, it will be returned automatically to the FTK interface, which will begin the FTK decryption process.

To perform auto-decryption, you must have PRTK or DNA 7.3 or higher installed on the same computer as the Examiner.

To auto decrypt files

1. In the *Examiner*, use the *Quick Filters* to select **Encrypted Files**.
2. Right-click an encrypted file and select **Auto Decrypt**.
   A password recovery job is then started in PRTK/DNA.
   The *Data Processing Status* dialog shows the process of the job.
   You can view the status in the PRTK/DNA UI as well.
   When the job is completed, the status displays the following message:
   “The password has been recovered; attempting to decrypt the file.”
3. In the Examiner, use the *Quick Filters* to select **Decrypted Files**.
   If the file was decrypted, it will show in the File List.

Recovering Unknown Passwords of Encrypted Files

You may find encrypted files with unknown passwords in your case.

See Identifying the Encrypted Files in a Case on page 185.

If you have a license, you can use AccessData Password Recovery Toolkit (PRTK) or Distributed Network Attack (DNA) to attempt to recover passwords for encrypted files. You can use PRTK or DNA in the following ways:

- As a stand-alone product
- As an integrated tool with the Examiner

About Recovering Passwords using the PRTK/DNA Integrated Tool with Examiner

Using PRTK/DNA integration, you can easily send encrypted files to PRTK/DNA to attempt to recover unknown passwords. These passwords can then be used with the decryption tools to decrypt the encrypted files.

See About Decrypting Files on page 181.

In order to use this PRTK/DNA integrated tool to recover passwords, you must install version 7.2 or higher of PRTK or the DNA host on the same computer as the Examiner. (You cannot install both PRTK and DNA on the same computer.

Important: When an item is sent to PRTK/DNA for automatic decryption, a dictionary is automatically generated based on the case's wordlist in FTK. This dictionary is used "As Is" in conjunction with the English dictionaries and "PRTK" profile to attempt password recovery on the selected item.

For details about PRTK/DNA, see the *PRTK/DNA User Guide*.

As a workflow, you can do the following:

- Identify encrypted files in your case.
  See Identifying the Encrypted Files in a Case on page 185.
- Using the Examiner, select and send encrypted files to PRTK/DNA.
- A password recovery job is started in PRTK/DNA for each file that you send.

  Important: PRTK is a resource-intensive application. If you send more than 3 files at a time, you may significantly reduce the resources available to the Examiner. Because DNA uses distributed jobs, you can send more files without impacting the Examiner.
- You view the PRTK/DNA interface to view the status and results of the password recovery jobs.
- After jobs have been run in PRTK/DNA, you can use PRTK/DNA to copy all of the recovered passwords to the clipboard.
  See Copying Recovered Passwords From PRTK/DNA to the Windows Clipboard on page 189.
- You can then use the list of passwords with the decryption tools to decrypt the encrypted files.
  See About Decrypting Files on page 181.

Recovering Passwords using the PRTK/DNA Integrated Tool

You can attempt to recovery unknown passwords for encrypted files in your case.

To Recover Passwords using the PRTK/DNA Integrated Tool with Examiner

1. Use the Examiner to identify encrypted files.
   See Identifying the Encrypted Files in a Case on page 185.
2. In the *File List,* select the files that you want to sent to PRTK/DNA.
3. Click **Tools** > **Send to PRTK/DNA for password recovery...**
   If this option is not active, then PRTK or DNA is not installed on the same computer as the Examiner.
4. In the Send Files to PRTK/DNA dialog, confirm the file or files that you want to send.
   The dialog will display if PRTK or DNA is installed on the computer and will be used.
5. Click OK.
6. Use the PRTK/DNA interface to view job status and results.
7. Copy the list of recovered passwords to use to decrypt files.

Copying Recovered Passwords From PRTK/DNA to the Windows Clipboard

You can copy the list of recovered passwords to the Windows clipboard. This can be useful is creating a list of known passwords for other uses. For example, if you are using AccessData Forensics Toolkit (FTK), you can use this list to decrypt files in in your FTK cases.

The passwords are copied in text format, one password per line.

To copy recovered passwords to the clipboard

1. Complete at least one password recovery job.
2. In the toolbar, click the

icon.
   The passwords are copied to the Windows clipboard.
3. Open a text editor and paste the list in the file.
4. Copy the list into the Passwords list.

Decrypting Other Encryption Types

Decrypting EFS

Understanding EFS

Versions of Windows developed for business environments from Windows 2000 onwards include the ability to encrypt files and folders. This feature is known as Encrypting File System (EFS). It is not supported in Windows XP Home Edition.

EFS files, as well as Microsoft® Office, and Lotus® Notes (NSF) files and folders can be decrypted. To do so, the password must already be known.

In Windows, EFS-encrypted files or folders can be viewed only by the user who encrypted them or by the user who is the authorized Recovery Agent. When the user logs in, encrypted files and folders are decrypted and the files are automatically displayed.

Note: There are certain files that cannot be encrypted, including system files; NTFS compressed files, and files in the [*drive*]:\[Windows_System_Root] and its subdirectories.

Important: When a user marks an encrypted file as privileged and that file is later decrypted, all associated data with the newly decrypted file are able to be found in an index search as hits. When a user attempts to view the hits in a different list, an error is displayed that the path is invalid.

Decrypting EFS Files and Folders

To find EFS passwords, export encrypted files and add them as jobs in PRTK or DNA. When passwords are found, you are ready to decrypt the encrypted files.

Requirements

Different versions of Windows OS have different requirements for decrypting EFS.

Windows 2000 and XP Systems Prior to SP1

EFS files on Windows 2000 prior to Service Pack 4 and Windows XP systems prior to Service Pack 1 are automatically decrypted. Simply select the **Decrypt EFS Files** option when adding evidence to a case and PRTK technology decrypts the EFS files.

Windows XP SP1 or Later

For systems running Windows XP Service Pack 1 or later, or Windows 2000 Service Pack 4 or later, the user's or the Recovery Agent's password is needed before the EFS files can be decrypted.

Decrypting EFS

To decrypt EFS

1. In a case, click **Tools > Decrypt Files**.
2. In the *Decrypt Files* dialog, if EFS had been detected in your evidence, the EFS option will be active.
3. Select the EFS.
4. In the *Decrypt Files* dialog, click **Set Passwords**.
5. Enter the password.
   See About the Encrypted File Passwords List on page 183.
6. Select **Attempt Blank Password** to decrypt files with no password, or whose password is blank.

   Note: EFS encrypted files in the case are automatically detected. Decrypt File Types will automatically be marked according to the file types found. Unselect any file types that you do not want to decrypt.

7. Choose one of the following:
   - Click **Decrypt** to begin the decryption process.
   - Click **Cancel** to abandon the decryption and return to the case.

   Note: The **Decrypt** button is disabled until at least one password is entered, or until **Attempt Blank Password** is marked.

8. When decryption is complete, click **Cancel** to return to the case.

Decrypting Microsoft Office Digital Rights Management (DRM) Protected Files

If your organization uses Windows Rights Management (RMS) to protect your Microsoft Office files, you can use the Examiner to decrypt them. If you are investigating Microsoft Office files from within your organization, this saves you time by decrypting and indexing DRM protected files in batch. By using this feature you no longer have to first export each document and then decrypt them individually with the RMS server.

Important: This feature only applies to files that are DRM protected from within your Domain. You cannot use this feature to decrypt files that are protected by other organization's RMS systems.

To decrypt DRM protected files, the following prerequisites must exist:

- Your *Examiner* computer and the Microsoft RMS server must be in the same domain.
- The *Examiner* computer must be able to authenticate with the RMS server. The machine activation happen when you first attempt to open or to protect a document for the first time.
- You must be logged into the *Examiner* computer with a Domain account that has Super User access to the Microsoft RMS server.

To Decrypt DRM Protected Office Files

1. In the *Examiner*, click **Tools > Decrypt Files**.
2. Click **Decrypt**.
3. Enter your RMS credentials.

Decrypting Dropbox DBX Files

Dropbox is a cloud-based storage system that can be configured to retain some files on your personal computer and sync whenever you connect to the Internet. Full contents of the Dropbox cannot be recovered at this time; however, you can decrypt dropbox database (DBX) files in order to view database contents and artifacts. Viewable data can include, but is not limited to:

- Host_id
- User display name
- List of files found in the Dropbox folder
- List of files deleted from the Dropbox folder, if any
- Email associated with the Dropbox account
- Path to where Dropbox resides on the imaged machine

To decrypt a Dropbox DBX file

1. Process the encrypted Dropbox DBX file as evidence.
2. When processing is complete, click **Tools > Decrypt Files**.
3. Enter the password for the Dropbox file.

   Note: Dropbox DBX files can only be decrypted if you have the password.

4. Click **Save Password**.
5. Click **Decrypt**.

To locate Dropbox account data

1. Decrypt the Dropbox DBX files.
2. In the *Explore* tab, expand the **config.dbx** database file.
3. Expand the **tables** folder.
4. Select the **config** folder.
5. Select the **rows...** item in the *File List* pane
   The data will populate in the *File Content* pane.

To locate Dropbox file lists

1. Decrypt the Dropbox DBX files.
2. In the *Explore* tab, expand the **filecache.dbx** database file.
3. Expand the **tables** folder.
4. Select the **file_journal** folder.
5. Select an item in the *File List* pane.
   The data will populate in the *File Content* pane.

To locate deleted Dropbox file lists, if available

1. Decrypt the Dropbox DBX files.
2. In the *Explore* tab, expand the **filecache.dbx** database file.
3. Expand the **tables** folder.
4. Select the **deleted_fileids** folder.

5. Select an item in the *File List* pane.
   The data will populate in the *File Content* pane.

Important: Be sure the *Quick Picks* arrow is not highlighted when performing the above tasks. This will make it so only the files within the specific folder you have selected appear in the File List pane.

Decrypting Lotus Notes Files

Lotus Notes stores files in a container called an NSF file. Both the NSF container file and the individual files and emails within the NSF file can be encrypted. To decrypt Lotus Notes files, you may need to first decrypt the NSF container file, and then decrypt its contents.

When an NSF file is created, Lotus Notes also creates a user.id file. Lotus Notes uses the user.id file to identify the user. You must have the user.id file to decrypt the NSF container file and to decrypt its contents.

Lotus Notes versions 7 through 8.5, including NSF and ODS formats 48 and 51 are supported.

To decrypt a Lotus Notes NSF file

1. Process the encrypted NSF file and its corresponding **user.id** file as evidence in the same case. When an NSF file is created, the **user.id** file is created at the same time. You need both files.
2. When processing is complete, click **Tools > Decrypt Files**.
3. Enter the password to the **user.id** file.

   Note: Some files do not have a password applied. In these cases, you should click **Attempt Blank Password.**

4. Click **Save Password**.
5. Enable **Lotus Notes (whole NSF)**.
6. Click **Decrypt**.

To decrypt Lotus Notes and emails

1. Process the encrypted notes and emails and the corresponding user.id file as evidence in the same case.
2. When processing is complete, click **Tools > Decrypt Files**.
3. Enter the password to the **user.id** file

   Note: Some files do not have a password applied. In these cases, you should click **Attempt Blank Password**.

4. Click **Save Password**.
5. Enable **Lotus Notes (notes/emails)**.
6. Click **Decrypt**.

Decrypting S/MIME Files

You can decrypt RSA standard PKCS7 S/MIME email items. This includes MBOX, DBX, RFC822, and some PST/EDB archives. You cannot decrypt PGP encrypted emails, Lotus Notes proprietary encryption, and items with S/MIME signatures — only the S/MIME encryption.

The Key files are PFX and PEM. The Key files are flagged and kept track of during processing in the same way as EFS and NSF key files.

To decrypt S/MIME

1. In a case, click **Tools > Decrypt Files.**
2. In the *Decrypt Files* dialog, click **Set Passwords**.
3. Enter the password.
   See About the Encrypted File Passwords List on page 183.
4. Mark **Attempt Blank Password** to decrypt files with no password, or whose password is blank.

   Note: S/MIME encrypted files in the case are automatically detected. Decrypt File Types will automatically be marked according to the file types found. Unselect any file types you wish not to decrypt.

5. Click **Decrypt** to begin the decryption process,

   Note: The **Decrypt** button is disabled until at least one password is entered, or until **Attempt Blank Password** is marked.

6. When decryption is complete, click **OK** to return to the case.

Decrypting Credant Files (Dell Data Protection | Encryption Server)

Credant encryption is file-based and works much like EFS. The Credant Decryption option in the tools menu is unavailable unless the image contains Credant encryption.

Credant version 7.7 is supported in both online and offline key bundle modes.

The integration allows two options for decryption: offline, and online. For a key bundle located on the user's local machine or network, use the offline option. For a key bundle located on a remote server within your network, use the online option.

The first time a user decrypts Credant files and provides the Credant server credentials, that information is encrypted and stored in the database. Later, if that user needs to decrypt Credant files in that or another case, the credentials field populates automatically.

The credentials are stored separately for each user, so while one user may have the credentials stored, others may not until the others have processed a case with Credant files that need to be decrypted.

Both the Online and Offline Credant Decryption dialog boxes have a Decryption Threads drop-down box. This dictates the total number of threads assigned to decryption, not the number of decryption threads per core. If you have a high-end system, you may benefit from a higher setting. At this time, it is not possible to cancel the processing once it has begun.

Important: If you click **Cancel** to process the evidence without decrypting, you will *not* be able to decrypt at a later time. Also, the evidence cannot be added to the same case a second time. You will have to create a new case to decrypt and process this evidence.

You can configure Credant server settings in the following ways:

- Globally, for all cases, in the *Case Manager* interface under the Tools menu.
- For a specific case. You can configure Credant decryption in one of the following ways:
  - When configuring Processing Options.

- On the *Additional Analysis* page
- On *Tools > Decrypt Files*

Important: This option uses an offline key bundle only. This method does not create any parent-child relationships, and as a result, produces fewer counts than the other methods of doing Credant decryption.

See Using an Offline Key Bundle on page 195.

Note: From the Processing Options or the Additional Analysis page, you can select to decrypt Credant files. If you select to decrypt Credant files, the File Signature Analysis option will automatically be selected as well.

See Using Additional Analysis on page 135.

You can now do a Live Search on Credant files on the fly after performing a drive preview.

Using an Offline Key Bundle

Offline decryption is a quicker and more convenient option if the key bundle can be placed on the investigator's local computer. To decrypt an encrypted image offline, select the key bundle file and enter the password used to decrypt it.

Important: This method does not create any parent-child relationships, and as a result, produces fewer counts than the other methods of doing Credant decryption.

To decrypt Credant files using an offline key bundle

1. Click **Tools > Credant Decryption** to open the *Credant Decryption Options* dialog.
2. Select the key bundle file by entering its location or browsing to it.
3. Enter the password.
4. Re-enter the password.
5. Click **OK**.

Using an Online Key Bundle

Online decryption can occur only when the computer processing the image can directly access the server over the network.

Usually the **Machine ID** and **Shield ID** fields are automatically populated. The **Machine ID** can be found on the server as the **Unique ID** on the **Properties** tab. The **Shield ID** can be found as the "Recovery ID" on the "Shield" tab. It looks similar to this: "ZE3HM8WW". If the Shield ID is not working, you have the option to use the **SDE Key ID**, which will auto-populate when available and should only be used after you have tried the Shield ID.

The Server Data group box contains information on how to contact the server. It includes the Credant Server user name, password, and IP address. The port should be 8081, and is auto-populated.

Offline decryption requires you to get a key bundle file from the server. Then, select the key bundle file and enter the password used to decrypt it. Get the key bundle file by executing the CFGetBundle.EXE file with a command like that looks like this:

```
CFGetBundle -Xhttps://10.1.1.131:8081/xapi -asuperadmin -Achangeit
-dxp1.accessdata.lab -sZE3HM8WW -oKeyBundle.bin -ipassword
```

-X for the server address

-a for administrator name

-A for the administrator password

-d for the Machine ID

-s for the Shield ID

-o for the output file

-i for the password used to encrypt the key bundle

Note: All command line switches are case sensitive. Also, as in the example above, there is no space between the switch and the accompanying data.

Once you have used either the online or the offline method, the files will be decrypted immediately and the decrypted file will become a child of the encrypted file. After decryption, the files will be processed with the same settings last used to process a file.

Once the key has been added and the appropriate partitions selected, click **OK** to return to the *Manage Evidence* dialog. Select a time zone from the Time Zone drop-down, then click **OK** to begin processing.

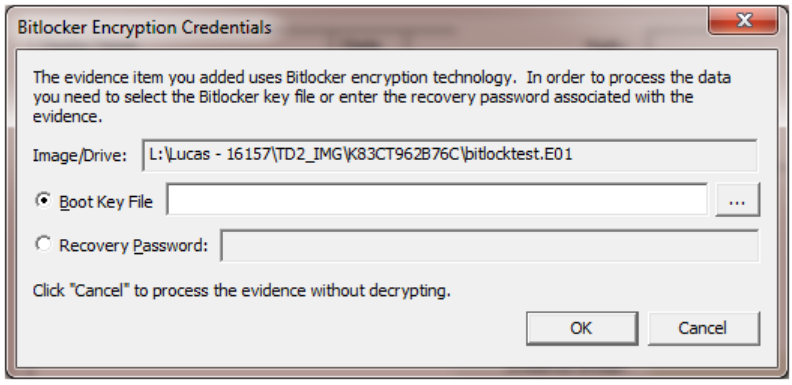
Important: If you click *Cancel* to process the evidence without decrypting, you will *not* be able to decrypt at a later time. Also, the evidence cannot be added to the same case a second time. You will have to create a new case to decrypt and process this evidence.

Decrypting Bitlocker Partitions

If you have the proper credentials, you can decrypt Bitlocker encrypted partitions. You can decrypt the Bitlocker partitions from Windows Vista and Windows 7 computers. You can provide the unique credentials for multiple encrypted partitions. After you provide Bitlocker credentials, files in the encrypted partitions are decrypted while the evidence is processed.

To decrypt Bitlocker partitions

1. Add evidence that has Bitlocker encryption to a case.
   If Bitlocker encryption is detected, you are prompted to enter credentials in the following dialog:



2. Enter one of the following credentials:
   - Boot Key File
   - Recovery Password.
3. If there are multiple partitions, a dialog will be displayed saying that the password for the first partition is valid, and that additional partitions remain encrypted.

4. Click **OK** and the credential dialog is again displayed for the next partition.
   This sequence continues until you have entered the credentials for all encrypted partitions.

Decrypting Safeguard Utimaco Files

You can use either Imager or the *Examiner* interface to decrypt boot drives that were encrypted with SafeGuard by Utimaco.

Safeguard Easy

Safeguard Easy works only with an image of a complete drive or a live drive. Imaged partitions cannot be decrypted because the information needed to decrypt the partition exists in the boot record of the drive.

When a live drive or drive image is added as evidence, it is checked to determine if SafeGuard Easy encryption is used on the drive. If it is used, a dialog will appear asking for the user name and password required to access the drive. If the correct user name and password are entered, the drive will be decrypted transparently during processing and the user can access information on the drive as though the drive were not encrypted. Incorrect passwords will result in long waits between attempts -- waits that grow exponentially for each failure. Hitting the cancel button on the dialog will allow the drive to be added as evidence, but the encrypted portions will not be processed.

Secondary hard drives and removable media that has been encrypted with SafeGuard Easy are not currently supported. The problem with secondary drives and removable media is that they contain NO information that indicates how they are encrypted. The encryption information for secondary drives and removable media is contained on the boot drive of the computer that encrypted them.

Versions 2.x and later, and all Imager versions since then support SafeGuard Easy drives encrypted with the following algorithms: AES128, AES256 (the default), DES, 3DES, and IDEA.

The Safeguard dialog box appears only when a valid Utimaco-encrypted image is read.

The username and password used to create the encrypted image are required for decryption. Once the credentials have been added, click **OK** to return to the *Manage Evidence* dialog. Select a time zone from the Time Zone drop-down, then click **OK** to begin processing.

Important: The following important information applies when using SafeGuard Decryption:

- Enter the User Name and Password carefully and verify both before clicking *OK*. If this information is entered incorrectly, the entire image is checked for matching information before returning with an error message. Each wrong entry results in a longer wait.
- If you click *Cancel* to process the evidence without decrypting, you will *not* be able to decrypt at a later time. Also, the evidence cannot be added to the same case a second time. You will have to create a new case to decrypt and process this evidence.

SafeGuard Enterprise

SafeGuard Enterprise (SGN) is supported. Utimaco supplied libraries to access the decryption keys for SGN via their recovery mechanism. This involves a somewhat cumbersome challenge/response system with the server to access the decryption keys. Each partition may be decrypted with a different key. The challenge/response process needs to be done for each encrypted partition. In order to enable the challenge/response system, a file called `recoverytoken.tok` needs to be retrieved from the server and selected in the decryption dialog. A recoverytoken.tok file is automatically selected if it is in the same directory as the evidence file.

SafeGuard Enterprise decryption was developed using version 5.x.

AccessData uses SafeGuard-provided `BE_Sgn_Api.DLL` and `BE_KBRDLLn.DLL`. These libraries are 32-bit libraries. The 32-bit process is used to retrieve keys in 64-bit. The actual decryption of the drive is done in the *Examiner*, but the SafeGuard libraries are needed to generate the key from the username/password.

To recognize that a drive is encrypted with SafeGuard Enterprise, “UTICRYPT” is searched for at the beginning of the first sector of each partition.

Retrieving the Recovery Token

Before the decryption process can occur, the `recoverytoken.tok` file must be retrieved from the server.

To retrieve the Recovery Token

1. From the server, you must create a virtual client.
2. Then you must export the virtual client. This is where the `recoverytoken.tok` file is created.
3. This file must be copied to a place where the *Examiner* can access the file.
4. Click the **Recovery** button next to each partition to retrieve that partition’s key. A dialog will open, telling you which key to retrieve:
   4a. On the server, select **Tools > Recovery** from the menu.
   4b. Select the virtual client you exported (the `recoverytoken.tok` file)
5. Select **Key requested.**
6. Find the requested key (in this case `0x1C3A799F48FB4B199903FB5730314ABF`). You can use **Find > Key IDs** from the drop-down, and enter a partial key into **Search Name** to help find the correct key.
7. A challenge code of 6 segments of 5 characters each is offered.
8. Enter the characters from the challenge portion of the dialog into the server’s dialog.
9. Click **Next**.
10. The server then offers a response code consisting of 12 segments of 5 characters each.
11. Enter these into the corresponding dialog that provides the decryption key.
12. Click **OK**. The drive is decrypted and added as evidence to the case.

Decrypting SafeBoot Files

SafeBoot is a program that encrypts drives and/or partitions. The encryption key must be available to enter into the **Key** field. All recognized partitions are selected by default, up to a maximum of eight. You can unselect any partition that you do not want to add to the case.

Important: The following important information applies when using SafeBoot Decryption:

- If you click **Cancel** to process the evidence without decrypting, you will *not* be able to decrypt at a later time. Also, the evidence cannot be added to the same case a second time. You will have to create a new case to decrypt and process this evidence.
- You must add all partitions and decrypt the encrypted partitions when first adding the evidence to the case or you will be unable to see them. Encrypted partitions do not display in the Evidence list.

Once the key has been added and the appropriate partitions selected, click **OK** to return to the *Manage Evidence* dialog. Select a time zone from the Time Zone drop-down, then click **OK** to begin processing.

Decrypting Guardian Edge Files

When a Guardian Edge-encrypted image is added to a case, it is automatically detected as a Guardian Edge image and a dialog will appear asking for credentials. The dialog has a drop-down list box with the user names that have been found to be associated with the image. Select the user name for which you have a password and enter that password. Enter the password in one of two ways:

- Enter it twice with dots appearing for each character (to keep it hidden from on-lookers).
- Check the **Show in plain text** box and enter it once.

Click **OK** to proceed with the decryption process.

Important: If you click **Cancel** to process the evidence without decrypting, you will *not* be able to decrypt at a later time. Also, the evidence cannot be added to the same case a second time. You will have to create a new case to decrypt and process this evidence.

Decrypting an Image Encrypted With PGP® WDE

You can acquire images from disks that have been protected with PGP® Whole Disk Encryption (WDE). This section describes the support for, and the process of specifying the credentials necessary to decrypt the image.

Note: Decryption is only possible if an existing credential, such as a user passphrase or a previously-configured Whole Disk Recovery Token, is available.

PGP® WDE Decryption

Individuals and organizations typically use PGP® Whole Disk Encryption (PGP® WDE) to protect the information on their laptop computers in case of loss or theft. Encrypted disks prompt for a user's passphrase before Windows loads, allowing data to be decrypted on the fly as it is read into memory or encrypted just before being written to disk. Disks remain encrypted at all times.

Administrators can instruct PGP® WDE devices that are managed by a PGP® Universal™ Server to automatically secure an encrypted disk to additional credentials based on a company's central policy. These could include a WDE Administrator key (for IT support purposes), an Additional Decryption Key (also called a corporate recovery key) and/or a Whole Disk Recovery Token ("WDRT"). WDRTs are commonly used to reset a forgotten passphrase and, can also be used by authorized administrators or examiners to decrypt an acquired image of a PGP® WDE encrypted drive.

To decrypt a PGPWDE Image and add it to a case

1. After creating a case, click **Evidence > Add / Remove Evidence > Add > Acquired Images > OK.**
2. Browse to the location of the image files and select the first of the set to add to this case.
3. You may enter any user's boot password or passphrase, or use the Whole Disk Recovery Token (WDRT) to decrypt a drive or image. Use one of the following methods:
   - *Boot passwords:* The users for the drive are displayed in the drop-down list in the PGP® Encryption Credentials box. Select the user and enter that user's boot password.
   - *Whole Disk Recovery Token (WDRT):* Obtain the WDRT by doing the following:

   3a. Log into the PGP® Universal™ Server.

   3b. Select the **Users** tab.

   3c. Click on the User Name having a recovery icon for the system being examined.

   3d. In the popup dialog in the far right column click the WDRT link to display information about the WDRT. The WDRT will look similar to this:

   ULB53-UD7A7-1C4QC-GPDZJ-CRNPA-X5A

   3e. You can enter the key, with or without the dashes, in the Passphrase/WDRT text field as the credential to decrypt a drive or image. The WDRT can be copied and pasted into the text field to avoid errors.

   3f. Click **OK**.

Important: If you click **Cancel** to process the evidence without decrypting, you will *not* be able to decrypt at a later time. Also, the evidence cannot be added to the same case a second time. You will have to create a new case to decrypt and process this evidence.

4. Verify that the PGP® WDE encrypted image is added to the case Manage Evidence list.

Viewing Decrypted Files

After you have decrypted files, you can view which files have been decrypted.

You can also view the *File Properties* of the original encrypted file to see the password that was used to decrypt that file.

To view decrypted files

1. Open the Examiner.
2. Do one of the following:
   - To use the Overview tab, do the following:

   2a. Click the **Overview** tab.

   2b. Expand **File Status**.

   2c. Click **Decrypted Files**

   - To use a filter, do the following:

   2a. Click the QuickPick icon for *Evidence* to view all or some of the of the evidence in the case.

   2b. Using the Filters drop-down menu, select **Decrypted Files**.

   In the *File List,* all decrypted files will be displayed.
3. Click on an individual file in the File List to view the file in the File Content pane.

Chapter 13

Exporting Data from the Examiner

This section discusses how to export data from the Examiner interface.

Copying Information from the Examiner

You can use the *Copy Special* dialog to copy information about the files in a case to the computer clipboard. The file information can include any or all column items, such as *Filename*, *File Path*, *File Category* etc. The data is copied in a tab-delimited format.

To copy file information

1. Select the files for the *Copy Special* task by doing either of the following:
   - In the *File List* on any tab, select the files that you want to copy information about.
   - Right-click the file in the file list.
2. Open the *Copy Special* dialog in any of these ways:
   - Select **Edit** > **Copy Special**.
   - Click the **Copy Special** button on the file list pane.
   - Click **Copy Special**.
3. In the *Copy Special* dialog, select from the following:

Item	Description
Choose Columns	Choose the column template definition that you want to use for the exported data.
Include Header Row	Includes a header row that uses the column headings you selected.
All Highlighted	Copies all items highlighted in the current file list.
All Checked	Copies all items checked in all file lists. You can check files in multiple lists. Checked items remain checked until you uncheck them.
Currently Listed	Copies all items in the current file list.
All	Copies all items in the case. Selecting this option can create a very large `TSV` or `CSV` file, and may exceed the 10,000 item capacity of the clipboard.

4. In the *Choose Columns* drop-down list, select the column template that contains the file information that you want to copy.

5. To define a new column settings template click *Column Settings* to open the *Column Settings Manager*.
6. Click **OK** to copy the data to the clipboard.

Exporting Files to a Native Format

You can export files that you find in an investigation to process and distribute to other parties. For example, you can export encrypted files that you need to decrypt with Password Recovery Toolkit (PRTK). You can also export Registry files to analyze in the Registry Viewer.

To export items from a case

1. Do either of the following:
   - In the *Examiner*, click **File** > **Export**
   - Right-click on a file in the *File List* pane and click **Export**
2. In the *Export* dialog, select from the following export options:

Export Options

File Options	Description
Append Item number to Filename	Adds the case's unique File ID to the filename of the exported item.
Append extension to filename if bad/absent	Uses the file's header information to add missing file extensions.
Export Children	Expands container-type files and exports their contents.
Exclude Slack Space Children Files	Excludes all slack files from the export.
Save HTML view (if available)	Saves applicable files in HTML format.
Export emails using Item number for name	Substitutes the Item number in the case instead of the email title to shorten the file paths.
Export directory as file	Creates a file that contains the binary data of a directory that you export. If you select a folder to export, the *Examiner* does not export the parent folder or empty sub-folders. You can export folders as files, but any empty folders that are not selected to be exported as files are not created during the export. To work around this issue, export a folder structure with its children, move up one folder level and mark *Export directory as file* and *Export children*.
Limit Path Length	The Limit Path Length option is now off by default. This prevents getting only partial paths in the export.
Create Manifest files	Generates manifest files that contain the details and options that are selected for the exported data. including headers. The Export Summary File is commonly called a Manifest file. If you select this option the export creates the manifest file CSV format. The export saves the file in the same destination folder as the exported files.

Export Options (Continued)

File Options	Description
Include original path	Includes the full path from the root to the file. The export maintains the folder structure for the exported files.
Export emails as MSG	Exports email files into the MSG format for broader compatibility.
Export emails to PST	Exports email files to a PST file. See Exporting Emails to PST on page 214.
Export messages from email to PST	You can export email messages to a PST file, even if they didn't come from a PST file originally. This lets you accomplish the following: ● Export messages from RFC822, NSF, PST, Exchange, and so on to a PST. ● As the opposite of reduction, you can create a new PST file with responsive messages in it. This creates a new PST rather than exporting the whole source PST and running reduction to remove anything non-responsive. ● Convert email archives, such as NSF, to a PST with the same folder and message structure. The Exporting Emails to PST feature requires that you have either Microsoft Outlook or the Microsoft Collaboration Data Objects (CDO) installed on the same computer as the processing engine. See the *Important Information* in the *Release Notes*.
Include thumbnails of video files	Includes the thumbnails of the video files that were created during evidence processing or during additional analysis.
Include common video format	Includes the common video format (MP4) files that were created during evidence processing or during additional analysis.

3. Select the items that you want to export from the following options:

Target Item	Description
All Checked	Selects all items checked in all file lists. You can check files in multiple lists.
All Listed	Selects all items in the current file list.
All Highlighted	Selects all items highlighted in the current file list. Items remain highlighted only as long as the same tab is displayed.
All	Selects all items in the case.

4. In the *Destination Base Path* field, enter or browse to and select the location to export the file.
   The default path is [*Drive*]:\case_folder\Report\Export\.
5. Click **OK**.

Exporting Files to an AD1 Image

You can export files to an Image. However; you can only export files to the AD1 format, or to their native format.

To export files to their native type see Exporting Files to a Native Format (page 204).

To export images into an image file Exporting an Image to an Image (page 208).

To export a file to an image

1. In the *Examiner*, do one of the following:
   - Highlight the items that you want to export.
   - Check the items that you want to export.
   - Make the *File List* pane display the items that you want to export.
2. Click **File > Export to Image**.
3. In the *Create Custom Content Image* dialog, select the appropriate option based on your decision in step one of this procedure Click **OK**.
4. In the *Create Image* dialog, under *Image Destination(s)*, click **Add**.
5. In the *Select Image Destination* dialog, specify the following information:

Image Options

Option	**Description**
Case Number	(Optional) Lets you enter a case number for the data that is to be exported.
Evidence Number	(Optional) Lets you enter an evidence number for the data that is to be exported.
Unique Description	(Optional) Lets you add a description to the data that is to be exported.
Examiner	(Optional) Lets you add the name of the evidence examiner to the data that is to be exported.
Notes	(Optional) Lets you add notes to the data that is to be exported.
Image Destination Type	Only AD1 is supported for unique file(s).
Relative to	The image can be saved locally (*Relative to This machine*), or remotely (*Relative to Remote source machine*).
Folder	Specify the path and the destination folder for the image on the target computer.
Username	Specify the domain and the user name to access the target computer.
Password	Specify the password of the user on the target computer.
Image Filename (Excluding Extensions)	Specify a filename for the image, but do not include an extension.
Image Fragment Size	Specify the image fragment size in MB. You can save RAW and E01 file types in a single segment by specifying 0 MB.

Image Options (Continued)

Option	**Description**
Compression	Specify the compression level to use. 0 represents no compression, 9 represents the highest compression. Compression level 1 is the fastest to create. Compression level 9 is the slowest to create.
Use AD Encryption	Select this option if you want to encrypt the image as it is created. When exporting data to an image from an encrypted drive, create the image physically, not logically. A physical image is often required for decrypting full disk encryption. AD Encryption supports the following: ● Hash algorithm SHA-512. ● Crypto algorithms AES 128, 192, and 256. ● Key materials (for encrypting the AES key): pass phrases, raw key files, and certificates. A raw key file is any arbitrary file whose raw data is treated as the key material. Certificates use public keys for encryption and corresponding private keys for decryption.

6. Click **OK**.

Exporting an Image to an Image

You can export images into the following types:

- AD1 (AD Custom Content)
- E01 (EnCase Compatible)
- S01 (Smart)
- 001 (RAW/DD)

To export case data to an image

1. In the *Examiner*, in the *Evidence Items* tree pane, select an image to export.
2. Click **File > Export to Image.**
3. In the *Create Custom Content Image* dialog, specify if you want to export the selected, highlighted, or checked items and then click **OK**.
4. In the *Create Image* dialog, under *Image Destination(s)*, click **Add**.
5. In the *Select Image Destination* dialog, specify the following information:

Image Destination Options

Option	**Description**
Case Number	(Optional) Lets you enter a case number for the data that is to be exported.
Evidence Number	(Optional) Lets you enter an evidence number for the data that is to be exported.
Unique Description	(Optional) Lets you add a description to the data that is to be exported.
Examiner	(Optional) Lets you add the name of the evidence examiner to the data that is to be exported.
Notes	(Optional) Lets you add notes to the data that is to be exported.
Image Destination Type	By default, the image type is AD1. When exporting to an AD1, the image's file path is added under a root directory. This behavior speeds the process of gathering data for the AD1, and shortens the path to the AD1 content.
Relative to	The image can be saved locally (*Relative to This machine*), or remotely (*Relative to Remote source machine*).
Folder	Specify the path and the destination folder for the image on the target computer.
Username	Specify the domain and the user name to access the target computer.
Password	Specify the password of the user on the target computer.
Image Filename (Excluding Extensions)	Specify a filename for the image, but do not include an extension.

Image Destination Options (Continued)

Option	**Description**
Image Fragment Size	Specify the image fragment size in MB. You can save RAW and E01 file types in a single segment by specifying 0 MB.
Compression	Specify the compression level to use. 0 represents no compression, 9 represents the highest compression. Compression level 1 is the fastest to create. Compression level 9 is the slowest to create.
Use AD Encryption	Select this option if you want to encrypt the image as it is created. When exporting data to an image from an encrypted drive, create the image physically, not logically. A physical image is often required for decrypting full disk encryption. AD Encryption supports the following: ● Hash algorithm SHA-512. ● Crypto algorithms AES 128, 192, and 256. ● Key materials (for encrypting the AES key): pass phrases, raw key files, and certificates. A raw key file is any arbitrary file whose raw data is treated as the key material. Certificates use public keys for encryption and corresponding private keys for decryption.

6. Click **OK**.
7. In the *Create Image* dialog, choose if you want to **Verify Images after they are created**.
8. Choose if you want to **Precalculate progress statistics**. This feature estimates the progress of the task as it is running.
9. Choose if you want to **Add image to case when completed**.
10. Specify the **Time Zone** of the evidence.
11. Click **OK**.
12. Click **Start**.

Exporting File List Information

You can use Copy Special functionality to save file list information into a file. You can save this file in TSV, TXT, CSV, or XML format. TXT files display in a text editor program like Notepad. Files saved in TSV, CSV, or XML can be opened in a spreadsheet program.

To export file list information to a network/folder/etc you must have rights to access and save information to the location.

To export File List information

1. Do one of the following:
   - In the *Examiner*, select **File** > **Export File List Info**.
   - Right-click on a file in the *File List* pane and select **Export File List Info.**
2. Select the items to export.
   Choose from:
   - **All Highlighted** (in the File List View)
   - **All Checked** (in the case)
   - **All Listed** (in the File List View)
   - **All** (in the case)
3. Specify if you want to include a header row in the exported file.
4. From the **Choose Columns** drop-down, select the column template to use. You can click **Column Settings** to create a column template to use for the export.
5. Specify the filename for the exported information.
6. Choose a file type for the exported file.
7. Browse to and select the destination folder for the exported file.
8. Click **Save**.

Exporting a Word List

You can export the contents of the case index or registry into a word list. You can use this word list as the basis for a custom dictionary to aid in the password recovery process.

You must have indexed the case to export the word list. If you have not indexed the case, you can click **Evidence > Additional Analysis**. In the *Additional Analysis* dialog, under *Search Indexes*, select **dtSearch Index**, and then click **OK**.

You can only export Registry Viewer contents into a word list if the Registry Viewer is installed on the computer where you are running the *Examiner*.

To export a word list

1. In the *Examiner*, select **File** > **Export Word List**.
2. Select the Registry keys that you want to include in the word list.
3. Click **Export**.
4. Click **Browse Folders** and select the filename and location for the exported word list.
5. Click **Save**.

Exporting Recycle Bin Index Contents

You can export the indexed data from INFO2 files into **TXT, TSV,** or **CSV** format.

To export INFO2 files

1. Locate an INFO2 file. In the *Examiner* you can find them in the *Overview* tab under **OS/File System Files > Recycle Bin Index**.
2. In the *File List*, highlight the INFO2 files that you want to export.
3. Right-click on the selected files and choose **Export Recycle Bin Index Contents**.
4. Browse to and select the desired destination folder.
5. Type a filename for the exported data file.
6. In the **Save as type** drop-down, select the file type to use.
7. Mark **Include header row** if you want the column headings included in the exported file.
8. Click **Save.**

Exporting Hashes from a Case

You can export hashes from a case. You can add the hash list into the Known File Filter in the same case to identify and set the KFF status on files of interest (Alert) or files of no interest (Ignore). You can use the Disregard status to make it easier to use existing groups, ignoring certain sets in the group that may have Alert status assigned.

To export hashes from the case

1. In the *Examiner*, in the *File List* view, select the files that you want to export the hashes for.
2. Right-click in the list and choose **Export File List Info**.
3. In the *Save As* dialog box, in the *File name* field, enter the name for the exported list.
4. In the *Save as type* drop-down, select either TSV or CSV.
5. Under *File List items to export*, select from the following:
   - All highlighted
   - All checked
   - Currently listed
   - All (In case)
6. Click **Choose Columns** and select the column settings to use.

   If you do not find the correct column setting for this export, click **Column Settings** to customize a column setting to include the file properties you want in this export.

   You should include MD5 Hash, and it is recommended that you also include SHA1 Hash. It is optional to include SHA 256 Hash.
7. In the *Selected Columns* list, double-click on each item to add and remove the columns.
8. Click **OK**.
9. Click **Save**.

Exporting KFF Data

You can use the KFF Admin interface to export KFF Data.

See Exporting KFF Data on page 296.

Exporting All Hits in a Search to a CSV file

After you run a search for terms, words, or predefined patterns, you can export your results to a comma delimited text file (CSV).

To Export All Hits in a Search to a CSV file

1. Run either a *Live Search* or an *Index Search*.
2. From either the *Index Search Results* window or the *Live Search Results* window, right click the search result and click **Set Context Data Width**.
3. Set the width value. For example, 32.
4. Right-click the search result and click **Export to File > All Hits in Search**.
5. In the *Save As* dialog, browse to the destination where you want to save the file.
6. In the *File Name* field, enter a name for the file.
7. In the *Save as type* field select *Comma Delimited Text File (*.CSV)*.
8. You can then import the CSV file into a program that supports CSV files such as Microsoft Excel.

Exporting Emails to PST

You can export email messages to a PST file, even if they didn't come from a PST file originally. This lets you accomplish the following:

- Export messages from RFC822, NSF, PST, Exchange, and so on to a PST.
- As the opposite of reduction, you can create a new PST file with responsive messages in it. This creates a new PST rather than exporting the whole source PST and running reduction to remove anything non-responsive.
- Convert email archives, such as NSF, to a PST with the same folder and message structure.

To export emails to PST

1. In the Export dialog, select **Export emails to PST**.
2. (Optional) If you want to preserve the folder structure, select **Preserve folder structure**.

   Note: When preserving the folder structure, the export creates a root directory for the email, followed by the user name associated with that email. The folder and message structure then mirror that of the emails being exported.

3. Select how you want to organize the exported emails.
   Choose from the following export options:
   - Separate PST per evidence.
   - Separate PST per custodian
   - Single PST
   - PST per mail archive
4. Configure other export options and click **OK.**

To convert email archives with the same folder and message structure

1. In the Export dialog, select **Export messages from email archives to PST**.
2. Configure other export options and click **OK.**

Exporting the Properties Panel

You can export the information in the properties panel to one of two options:

- CSV
- XML and HTML (these are exported at the same time)

To Export the Properties Panel Information to CSV:

1. Right-click anywhere inside the Properties Panel.
2. Select **Export to CSV**.
3. Select a *Destination Folder* and create a *File Name*.
4. Navigate to the newly-created file. When you open it, a *Text Import Wizard* will open. Be sure to select the following options:
   - Delimited
   - Comma

To Export the Properties Panel Information to XML and HTML:

1. Right-click anywhere inside the Properties Panel.
2. Select **Export to XML and HTML**.
3. Select a *Destination Folder* and create a *File Name*.
4. Navigate to the newly-created file. When you open it, be sure to select the **Open the file with the following style sheet applied** option and apply the **ADObjectProperties.xslt** style sheet. Once you have applied the stylesheet, the file may open in a web browser.

Exporting Geolocation Data to KML or KMZ

Geolocation data can be exported in order to allow users to view geolocation data from the case in any application that allows KML imports. For example, Google Earth.

To Export Geolocation Data:

1. Select the files for export from the file pane.
   This can be done using either of the following options:
   - Highlight one or more items (use the columns to sort photos based on attributes)
   - Select individual files by checking the box
2. Right-click on any of the selected files and click **Export File List Info**. A window will open, allowing you to select where to save the files and to determine which type of file you would like to export.

   Note: A KMZ file is a compressed KML file.

   Be sure to set the *Choose Columns* dropdown option to **Geolocation**.
3. Click **Save**.

To Open Geolocation Data in Google Earth:

1. Open the Google Earth program.
2. Drag and drop the KML or KMZ file onto the program.
   The pins will automatically populate on the map and will use the original file name.
3. The Google Earth program will change the icon for the KML or KMZ file to a Google Earth symbol.

   Note: The same process can be followed using Google maps; however, the KML or KMZ file will not be updated with a Google Earth icon.

Chapter 14

About Cerberus Malware Analysis

About Cerberus Malware Analysis

Cerberus lets you do a malware analysis on executable binaries. You can use Cerberus to analyze executable binaries that are on a disk, on a network share, or that are unpacked in system memory.

Cerberus consists of the following stages of analysis

- Stage 1: Threat Analysis

  Cerberus stage 1 is a general file and metadata analysis that quickly examines an executable binary file for common attributes it may possess. It identifies potentially malicious code and generates and assigns a threat score to the executable binary.

  See About Cerberus Stage 1 Threat Analysis on page 218.

- Stage 2: Static Analysis

  Cerberus stage 2 is a disassembly analysis that takes more time to examine the details of the code within the file. It learns the capabilities of the binary without running the actual executable.

  See About Cerberus Stage 2 Static Analysis on page 224.

Cerberus first runs the Stage 1 threat analysis. After it completes Stage 1 analysis, it will then automatically run a static analysis against binaries that have a threat score that is higher than the designated threshold.

Cerberus analysis may slow down the speed of your overall processing.

Note: This feature is available depending on your license. Please contact your sales representative for more information.

Important: Cerberus writes binaries to the AD Temp folder momentarily in order to perform the malware analysis. Upon completion it will quickly delete the binary. It is important to ensure that your antivirus is not scanning the AD Temp folder. If antivirus deletes/Quarantines the binary from the temp Cerberus analysis will not be performed.

Cerberus analyzes the following types of files:

acm	com	dll	exe	lex	ocx	scr	tlb
ax	cpl	dll~	iec	mui	pyd	so	tmp
cnv	dat	drv	ime	new	rll	sys	tsp
							wpc

About Cerberus Stage 1 Threat Analysis

Cerberus stage 1 analysis is a general analysis for executable binaries. The Stage 1 analysis engine scans through the binary looking for malicious artifacts. It examines several attributes from the file's metadata and file information to determine its potential to contain malicious code within it. For each attribute, if the condition exists, Cerberus assigns a score to the file. The sum of all of the file's scores is the file's total threat score.

More serious attributes have higher positive scores, such as +20 or +30. Safer attributes have smaller or even negative numbers such as +5, -10 or -20.

The existence of any particular attribute does not necessarily indicate a threat. However, if a file contains several attributes, then the file will have a higher sum score which may indicate that the executable binary may warrant further investigation. The higher the threat score, the more likely a file may be to contain malicious code.

For example, you may have a file that had four attributes discovered. Those attributes may have scores of +10, +20, +20, and +30 for a sum of +80. You may have another file with four attributes of scores of +5, +10, -10, -20 for a sum of -15. The first file has a much higher risk than the second file.

Cerberus stage 1 analysis also examines each file's properties and provides information such as its size, version information, signature etc.

About Cerberus Score Weighting

There are default scores for each attribute of Cerberus Stage 1 threat scoring. However, you can modify the scoring so that you can weigh the threat score attributes with your own values.

For example, the Bad Signed attribute as a default value of +20. You can give it a different weight of +30.

You must configure these scores before the files are analyzed.

About Cerberus Override Scores

Some threat attributes have override scores. If a file has one of these attributes, instead of the score being the sum of the other attributes, the score is overridden with a set value of 100 or -100. This is useful in quickly identifying files that are automatically considered either as a threat or safe. If a bad artifact is found that requires immediate attention, the file is given the maximum score. If an artifact is found that is considered safe, the file is automatically given the minimum score.

Score ranges have maximum and minimum values of -100 to 100.

- High threat signatures will result in a final score of 100.
- Low threat signatures will result in a final score of -100.

Cerberus attributes that that have maximum override scores include:

- Bad signatures
- Revoked signatures
- Expired signatures
- Packed with known signature

If any of these attributes are found, the score is overridden with a score of +100.

Cerberus Minimum override score includes:

- Valid digital signature

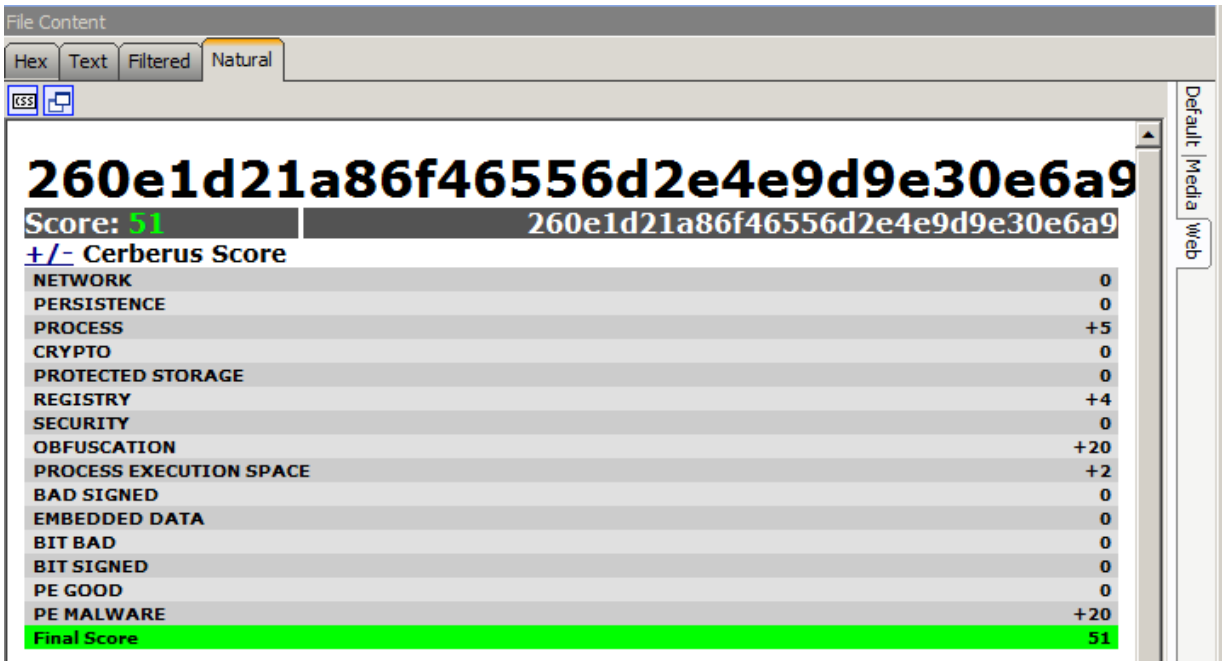
If this attribute is found, the score is overridden with a score of -100.

Important: If a file that is malware has a valid digital signature, the override will score the file as -100 (low threat), even though the file is really malware.

About Cerberus Threat Score Reports

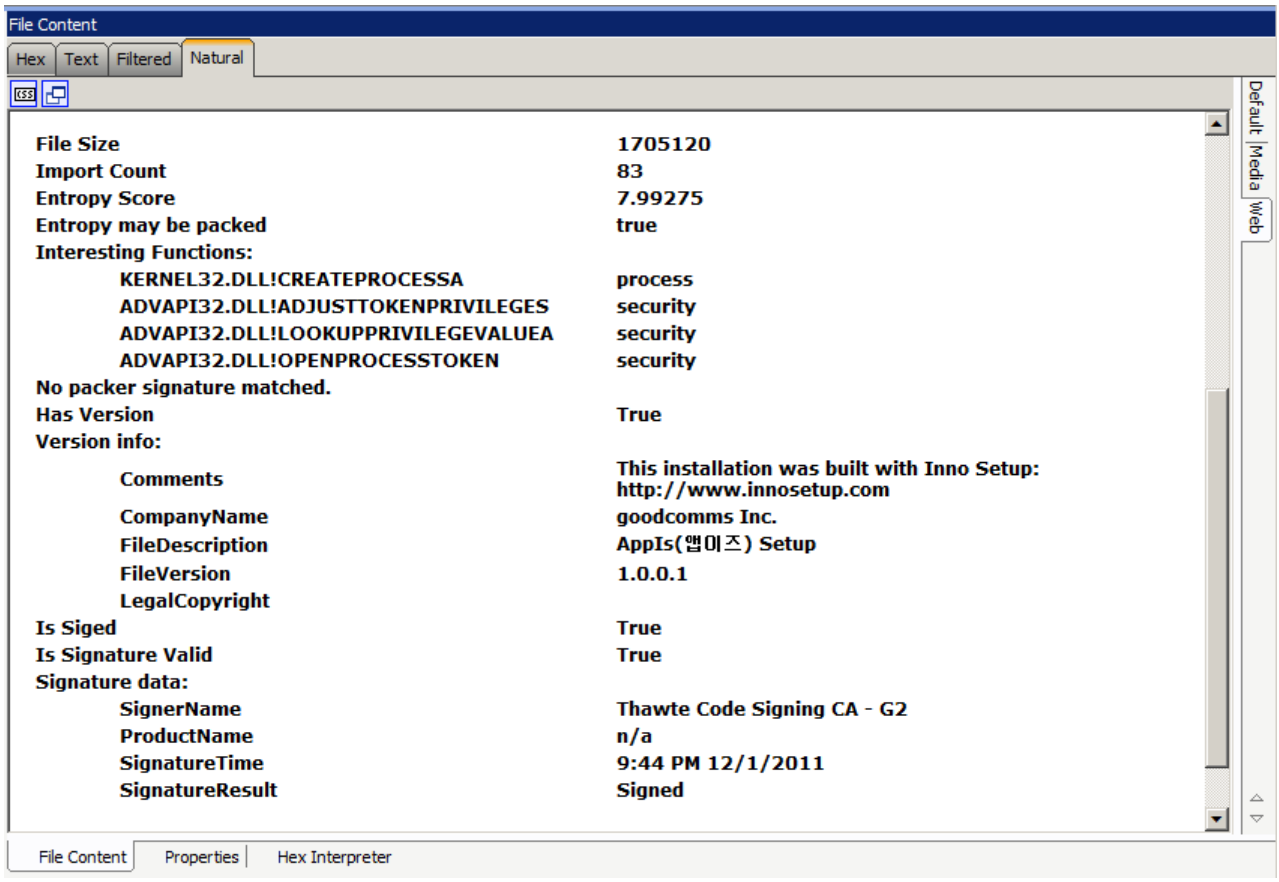
After you you have processed evidence with Cerberus enabled, you can view a threat score report for each executable file in a threat score reports. This report shows the Cerberus score that were calculated during processing. There are two columns of scores: the weighted score assigned to each attribute (the potential score) and the actual score given if the attribute was found in the file.

Cerberus Threat Score Report



The report also shows general file properties.

File Information Threat Score Report


File Content
Hex
Text
Filtered
Natural
Default
Media
Web
File Size 1705120
Import Count 83
Entropy Score 7.99275
Entropy may be packed true
Interesting Functions:
KERNEL32.DLL!CREATEPROCESSA process
ADVAPI32.DLL!ADJUSTTOKENPRIVILEGES security
ADVAPI32.DLL!LOOKUPPRIVILEGEVALUEA security
ADVAPI32.DLL!OPENPROCESSTOKEN security
No packer signature matched.
Has Version True
Version info:
Comments This installation was built with Inno Setup: http://www.innosetup.com
CompanyName goodcomms Inc.
FileDescription AppIs(앱이즈) Setup
FileVersion 1.0.0.1
LegalCopyright
Is Siged True
Is Signature Valid True
Signature data:
SignerName Thawte Code Signing CA - G2
ProductName n/a
SignatureTime 9:44 PM 12/1/2011
SignatureResult Signed
File Content
Properties
Hex Interpreter

Cerberus Stage 1 Threat Scores

The following table lists the threat scores that are provided in a Stage 1 analysis:

Cerberus Stage 1 Threat Score Attributes

Attribute	Default Threat Score	Description
Network	+5	The Network category is triggered when a program contains the functionality to access a network. This could involve any kind of protocol from high-level HTTP to a custom protocol written using low-level raw sockets.
Persistence	+20	Persistence indicates that the application may try to persist permanently on the host. For example, the application would resume operation automatically even if the machine were rebooted.
Process	+5	Process indicates the application may start a new a process or attempt to gain access to inspect or modify other processes. Malicious applications attempt to gain access to other processes to obfuscate their functionality or attack vector or for many other reasons. For example, reading or writing into a process's memory, or injecting code into another process.
Crypto	+6	Crypto is triggered when an application appears to use cryptographic functionality. Malicious software uses cryptography to hide data or activity from network monitors, anti-virus products, and investigators.
Protected Storage	+10	ProtectedStorage indicates that the application may make use of the Windows "pstore" functionality. This is used on some versions of Windows to store encrypted data on the system. For example, Internet Explorer stores a database for form-filling in protected storage.
Registry	+5	Registry is triggered when a target application attempts to use the registry to store data. The registry is commonly used to store application settings, auto-run keys, and other data that the application wants to store permanently but not in its own file.
Security	+5	Imports functions used to modify user tokens. For example, attempting to clone a security token to impersonate another logged on user.
Obfuscation	+30	Stage 1 searches for signs that the application is 'packed', or obfuscated in a way that hinders quick inspection. The Obfuscation category is triggered when the application appears to be packed, encrypted, or otherwise obfuscated. This represents a deliberate decision on behalf of the developer to hinder analysis.
Process Execution Space	+2	Unusual activity in the Process Execution Space header. For example, a zero length raw section, unrealistic linker time, or the file size doesn't match the Process Execution Space header.

Cerberus Stage 1 Threat Score Attributes (Continued)

Attribute	Default Threat Score	Description
Bad Signed	+20	This category is triggered when a binary is cryptographically signed, but the signature is invalid. A signature is generally used to demonstrate that some entity you trust (like a government or legitimate company, called a 'signing authority') has verified the authorship and good intentions of the signed application. However, signatures can be revoked and they can expire, meaning that the signature no longer represents that the signing authority has trust in the application.
Embedded Data	+10	This category is triggered when an application contains embedded executable code. While all programs contain some program code, this category indicates that the application has an embedded 'resource', which contains code separate from the code which runs normally as part of the application.
Bad / Bit-Bad	+20	This category is triggered when the application contains signatures indicating it uses the IRC protocol or shellcode signature. Many malware networks use IRC to communicate between the infected hosts and the command-and-control servers.
Signed / Bit Signed	-20	This category is triggered when a program is signed. A program that is signed is verified as 'trusted' by a third party, usually a legitimate entity like a government or trusted company. The signature may be expired or invalid though; check the 'BadSigned' category for this information.
PE Good	-10	Scores for good artifacts in PE headers.
PE Malware	+30	Scores for known malware artifacts in PE headers.

Cerberus Stage 1 File Information

The following table lists the threat scores that are provided in a Stage 1 analysis:

File Information from Cerberus Stage 1 Analysis

Item	Description
File Size	Displays the size of the file in bytes.
Import Count	Displays the number of functions that Cerberus examined.
Entropy Score	Displays a score of the binaries entropy used for suspected packing or encrypting.
Entropy may be packed	New:
Interesting Functions	Displays the name of functions from the process execution space that contributed to the file's threat score.
Suspected Packer List	Attempts to display a list of suspected packers whose signature matches known malware packers.
Modules	Displays the DLL files included in the binary.
Has Version	Displays whether or not the file has a version number.
Version Info	Displays information about the file that is gathered from the Windows API including the following: • CompanyName • FileDescription • FileVersion • InternalName • LegalCopyright • LegalTrademarks • OriginalFilename • ProductName • ProductVersion
Is Signed	Displays whether or not the file is signed. If the file is signed the following information is also provided: • IsValid • SignerName • ProductName • SignatureTime • SignatureResult
Unpacker results	Attempts to show if and which packers were used in the binary.

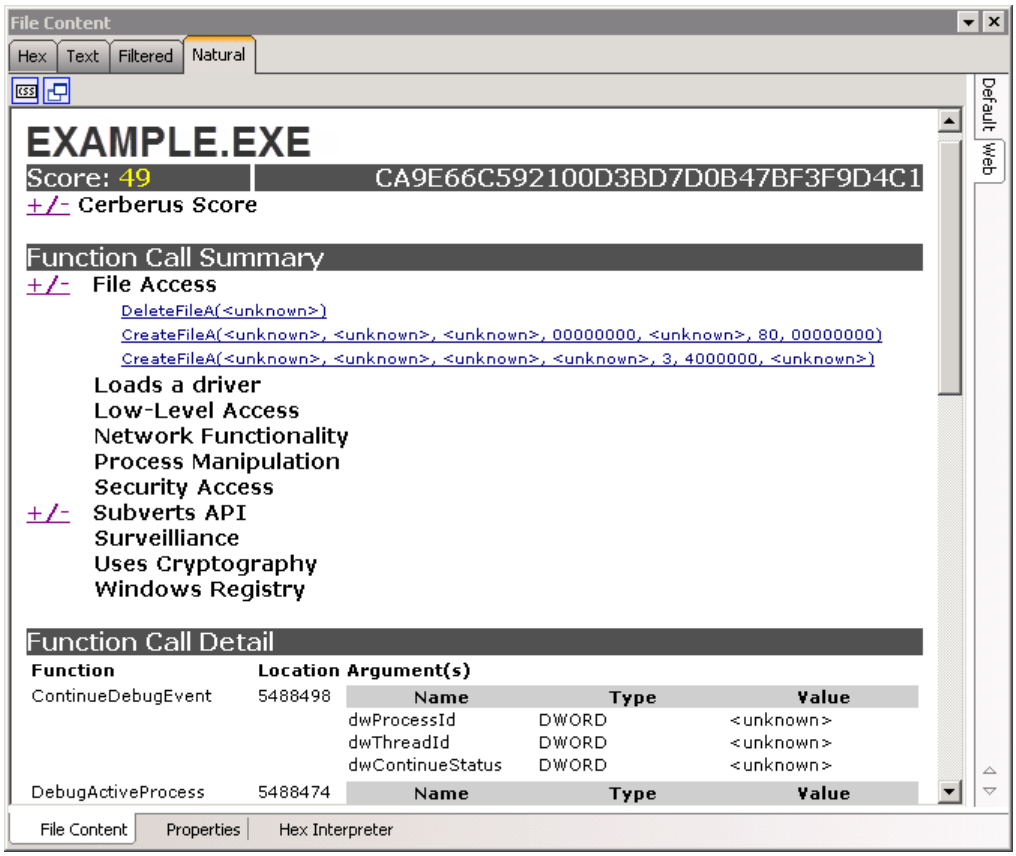
About Cerberus Stage 2 Static Analysis

When you run a stage 1 analysis, you configure a score that will launch a Cerberus stage 2 analysis. If an executable receives a score that is equal or higher than the configured score, Cerberus stage 2 is performed. Cerberus stage 2 disassembles the code of an executable binary without running the actual executable.

About Cerberus Stage 2 Report Data

When a stage 2 analysis runs, it returns its results of the file's functions in the Functional Call Summary section of the threat score report.

Cerberus Stage 2 Report Data in Threat Scan Report



Cerberus Stage 2 Function Call Data

Stage 2 analysis data is generated for the following function call categories:

- File Access
- Networking functionality
- Process Manipulation
- Security Access
- Windows Registry
- Surveillance
- Uses Cryptography
- Low-level Access
- Loads a driver
- Subverts API
- Misc

File Access Call Categories

Cerberus Stage 2 File Access Function Call Categories

Category		Description
File Access	Functions that manipulate (read, write, delete, modify) files on the local file system.	
	Filesystem.File.Read. ExecutableExtension	This is triggered by functionality which reads executable files from disk. The executable code can then be executed, obfuscated, stored elsewhere, transmitted, or otherwise manipulated.
	FileSystem.Physical. Read	This application may attempt to read data directly from disk, bypassing the filesystem layer. This is very uncommon in normal applications, and may indicate subversive activity.
	FileSystem.Physical. Write	This application may attempt to write data directly to disk, bypassing the filesystem layer in the operating system. This is very uncommon in normal applications, and may indicate subversive activity. It is also easy to do incorrectly, so this may help explain any system instability seen on the host.
	FileSystem.Directory. Create:	This indicates the application may attempt to create directory. Modifications to the file system are useful for diagnosing how an application persists, where its code and data are stored, and other useful information.
	FileSystem.Directory. Create.Windows:	This indicates an application may try to create a directory in the \Windows directory. This directory contains important operating system files, and legitimate applications rarely need to access it.
	FileSystem.Directory. Recursion:	This indicates the application may attempt to recurse through the file system, perhaps as part of a search functionality.
	FileSystem.Delete:	This indicates the application may delete files. With sufficient permissions, the application may be able to delete files which it did not write or even system files which could affect system stability.
	FileSystem.File.Delete .Windows:	This indicates the application may try to delete files in the \Windows directory, where important system files are stored. This is rarely necessary for legitimate applications, so this is a strong indicator of suspicious activity.
	FileSystem.File.Delete . System32:	This indicates the application may try to delete files in the \Windows\System32 directory, where important system files are stored. This is rarely necessary for legitimate applications, so this is a strong indicator of suspicious activity.
	FileSystem.File.Read. Windows:	This indicates the application may attempt to read from the \Windows directory, which is very uncommon for legitimate applications. \Windows is where many important system files are stored.
	FileSystem.File.Write. Windows:	This indicates the application may attempt to write to the \Windows directory, which is very uncommon for legitimate applications. \Windows is where many important system files are stored.

Cerberus Stage 2 File Access Function Call Categories (Continued)

Category		Description
	FileSystem.File.Read.System32:	This indicates the application may attempt to read from the \Windows\System32 directory, which is very uncommon for legitimate applications. \Windows\System32 is where many important system files are stored.
	FileSystem.File.Write.System32:	This indicates the application may attempt to write to the \Windows\System32 directory, which is very uncommon for legitimate applications. \Windows\System32 is where many important system files are stored.
	FileSystem.File.Write.ExecutableExtension:	This indicates the application may attempt to write an executable file to disk. This could indicate malicious software that has multiple ‘stages’, or it could indicate a persistence mechanism used by malware (i.e. write an executable file into the startup folder so it is run when the system starts up).
	FileSystem.File.Filename.Compression:	This indicates the program may write compressed files to disk. Compression can be useful to obfuscate strings or other data from quick, automated searches of every file on a filesystem.
	FileSystem.File.Filename.Autorun:	This indicates the application may write a program to a directory so that it will run every time the system starts up. This is a useful persistence mechanism.

Networking Functionality Call Categories

Cerberus Stage 2 Networking Functionality Function Call Categories

Category		Description
Networking functionality	Functions that enable sending and receiving data over the or other networks.	
	Network.FTP.Get:	Describes the use of FTP to retrieve files. This could indicate the vector a malware application uses to retrieve data from a C&C server.
	Network.Raw:	Functions in this category indicate use of the basic networking commands used to establish TCP, UDP, or other types of connections to other machines. Programmers who use these build their own communication protocol over TCP (or UDP or other protocol below the application layer) rather than using an application-layer protocol such as HTTP or FTP.
	Network.Raw.Listen:	Functionality in this category indicates the application accepts incoming connections over tcp, udp, or other lower-level protocol.
	Network.Raw. Receive:	Functionality in this bucket indicates that the application receives data using a socket communicating over a lower-level protocol such as TCP, UDP, or a custom protocol.
	Network.DNS.Lookup. Country.XX:	This indicates the application may attempt to resolve the address of machines in one of several countries. “XX” will be replaced by the ‘top level domain’, or TLD associated with the lookup, indicating the application may attempt to establish contact with a host in one of these countries.
	Network.HTTP.Read:	The application may attempt to read data over the network using the HTTP protocol. This protocol is commonly used by malware so that its malicious traffic appears to ‘blend in’ with legitimate web traffic.
	Network.HTTP. Connect.Nonstandard. Request:	This indicates the application may make an HTTP request which is not a head, get, or post request. The vast majority of web applications use one or more of these 3 kinds of requests, so this category indicates anomalous behavior.
	Network.HTTP. Connect.Nonstandard. Port:	Port: Most HTTP connections occur over either port 80 or 443. This indicates the application is communicating with the server over a non-standard port, which may be a sign that the server is not a normal, legitimate web server.
	Network.HTTP. Connect.Nonstandard. Header:	HTTP messages are partially composed of key-value pairs of strings which the receiver will need to properly handle the message. This indicates the application includes non-standard or very unusual header key-value pairs.
	Network.HTTP.Post:	This indicates the application makes a ‘post’ http request. ‘post’ messages are normally used to push data to a server, but malware may not honor this convention.

Cerberus Stage 2 Networking Functionality Function Call Categories (Continued)

Category		Description
	Network.HTTP.Head:	This indicates the application makes a ‘head http request. ‘head’ messages are normally used to determine information about a server’s state before sending a huge amount of data across the network, but malware may not honor this convention.
	Network.Connect. Country.XX:	This indicates the application may attempt to connect to a machines in one of several countries. “XX” will be replaced by the ‘top level domain’, or TLD associated with the lookup.
	FTP.Put:	The application may attempt to send files over the network using FTP. This may indicate an exfiltration mechanism used by malware.

Process Manipulation Call Categories

Cerberus Stage 2 Process Manipulation Function Call Categories

Category		Description
Process Manipulation	May contain functions to manipulate processes.	
	ProcessManagement.Enumeration:	This functionality indicates the application enumerates all processes. This could be part of a system survey or other attempt to contain information about the host.
	ProcessManagement.Thread.Create:	This indicates the target application may create multiple threads of execution. This can give insight into how the application operates, operating multiple pieces of functionality in parallel.
	ProcessManagement.Thread.Create.Suspended:	This indicates the application may create threads in a suspended state. Similar to suspended processes, this may indicate that the threads are only executed some time after they're created or that some properties are modified after they are created.
	ProcessManagement.Thread.Create:	This indicates the application may attempt to create a thread in another process. This is a common malware mechanism for 'hijacking' other legitimate processes, disguising the fact that malware is on the machine.
	ProcessManagement.Thread.Create.Remote:	This indicates that the application may create threads in other processes such that they start in a suspended state. Thus their functionality or other properties can be modified before they begin executing.
	ProcessManagement.Thread.Open:	The application may try to gain access to observe or modify a thread. This behavior can give insight into how threads interact to affect the host.
	ProcessManagement.Process.Open:	This application may attempt to gain access to observe or modify other processes. This can give strong insight into how the application interacts with system and what other processes it may try to subvert.
	ProcessManagement.Process.Create:	This application may attempt to create one or more other processes. Similar to threads, multiple processes can be used to parallelize an application's functionality. Understanding that processes are used rather than threads can shed insight on how an application accomplishes its goals.
	ProcessManagement.Process.Create.Suspended:	Describes functionality to create new processes in a suspended state. Processes can be created in a 'suspended' state so that none of the threads execute until it is resumed. While a process is suspended, the creating process may be able to substantially modify its behavior or other properties.

Security Access Call Categories

Cerberus Stage 2 Security Access Function Call Categories

Category		Description
Security Access	Functions that allow the program to change its security settings or impersonate other logged on users.	
	Security:	This category indicates use of any of a large number of security-related functions, including those manipulating security tokens, Access Control Entries, and other items. Even without using an exploit, modification of security settings can enable a malicious application to gain more privileges on a system than it would otherwise have.

Windows Registry Call Categories

Cerberus Stage 2 Windows Registry Function Call Categories

Category		Description
Windows Registry	Functions that manipulate (read, write, delete, modify) the local Windows registry. This also includes the ability to modify autoruns to persist a binary across boots.	
	Registry.Key.Create:	The application may attempt to create a new key in the registry. Keys are commonly used to persist settings and other configuration information, but other data can be stored as well.
	Registry.Key.Delete:	Registry.Key.Delete: This application may attempt to delete a key from the registry. While it is common to delete only keys that the application itself created, with sufficient permissions, Windows may not prevent an application from deleting other applications' keys as well.
	Registry.Key.Autorun:	This indicates the application may use the registry to try to ensure it or another application is run automatically on system startup. This is a common way to ensure that a program continues to run even after a machine is restarted.
	Registry.Value.Delete:	This indicates the application may attempt to delete the value associated with a particular key. As with the deletion of a key, this may not represent malicious activity so long as the application only deletes its own keys' values.
	Registry.Value.Set:	The application may attempt to set a value in the registry. This may represent malicious behavior if the value is set in a system key or the key of another application.
	Registry.Value.Set.Binary:	This indicates the application may store binary data in the registry. This data could be encrypted, compressed, or otherwise is not plain text.

Cerberus Stage 2 Windows Registry Function Call Categories (Continued)

Category		Description
	Registry.Value.Set.Text:	This indicates the application may write plain text to the registry. While the 'text' flag may be set, this does not mandate that the application write human-readable text to the registry.
	Registry.Value.Set.Autorun:	The application may set a value indicating it will use the registry to persist on the machine even after it restarts.

Surveillance Call Categories

Cerberus Stage 2 Surveillance Function Call Categories

Category		Description
Surveillance	Usage of functions that provide audio/video monitoring, keylogging, etc.	
	Driver.Setup:	Functionality in this category involves manipulation of INF files, logging, and other driver-related tasks. Drivers are used to gain complete control over a system, potentially even gaining control of other security products.
	Driver.DirectLoad:	Functionality in this category involves loading drivers. As noted in 'driver.setup', drivers represent ultimate control over a host system and should be extremely trustworthy.

Uses Cryptography Call Categories

Cerberus Stage 2 Uses Cryptography Function Call Categories

Category		Description
Uses Cryptography	Usage of the Microsoft CryptoAPI functions.	
	Crypto.Hash.Compute:	This indicates a hash function may be used by the target application. Hash functions are used to verify the integrity of communications or files to ensure they were not tampered with.
	Crypto.Algorithm.XX:	The "XX" could be any of several values, including 'md5', 'sha-1', or 'sha-256'. These represent particular kinds of hashes which the target application may use.
	Crypto.MagicValue:	This indicates that the target contains strings associated with cryptographic functionality. Even if the application does not use Windows OS functionality to use cryptography, the 'magic values' will exist so long as the target uses standard cryptographic algorithms.

Low-level Access Call Categories

Cerberus Stage 2 Low-level Access Function Call Categories

Category		Description
Low-level Access	Functions that access low-level operating system resources, for example reading sectors directly from disk.	
	Driver.Setup:	Functionality in this category involves manipulation of INF files, logging, and other driver-related tasks. Drivers are used to gain complete control over a system, potentially even gaining control of other security products.
	Driver.DirectLoad:	Functionality in this category involves loading drivers. As noted in ‘driver.setup’, drivers represent ultimate control over a host system and should be extremely trustworthy.
	Debugging.dbghelp:	This indicates use of functionality included in the dbghelp.dll module from the "Debugging Tools for Windows" package from Microsoft. With the proper permissions, the functionality in this library represents a power mechanism for disguising activity from investigators or for gaining control of other processes.
	Misc.SystemRestore:	Describes functionality involved in the System Restore feature, including removing and adding restore points. Restore points are often used as part of a malware-removal strategy, so removal of arbitrary restore points, especially without user interaction, may represent malicious activity.
	Debugging. ChecksForDebugger:	This is triggered if the application tries to determine whether it is being debugged. Malicious applications commonly try to determine whether they’re being analyzed so that they can modify the behavior seen by analysts, making it difficult to discover their true functionality.

Loads a driver Call Categories

Cerberus Stage 2 Loads a driver Function Call Categories

Category	Description
Loads a driver	Functions that load drivers into a running system.

Subverts API Call Categories

Cerberus Stage 2 Subverts API Function Call Categories

Category	Description
Subverts API	Undocumented API functions, or unsanctioned usage of Windows APIs (for example, using native API calls).

Chapter 15

Running Cerberus Malware Analysis

This chapter includes the following topics about running Cerberus in FTK-based products.

- About Reviewing Results of Cerberus (page 237)
- Using Index Search with Cerberus (page 240)
- Exporting a Cerberus Report (page 240)

Running Cerberus Analysis

Cerberus Analysis consists of two stages of analysis that help you to locate potentially malicious files. You can enable this analysis when creating a case or using *Additional Analysis*.

See About Cerberus Malware Analysis on page 217.

Stage 1 is called a threat analysis and quickly examines an executable binary file for common attributes it may possess. Stage 2 is called static analysis. Static analysis is a disassembly analysis that takes more time to examine the details of the code within the file.

For more information see About Cerberus Malware Analysis (page 217)

Cerberus first runs a threat analysis. After it completes Stage 1 analysis, it can then automatically run a static analysis against binaries with a threat score that is higher than a certain threshold.

Cerberus analysis may slow down the speed of your overall processing. Depending on the size of your data set and the amount of executable binaries that you must examine, it may be advisable to run Cerberus analysis in two steps after you complete initial case processing. In this case, you can first only run Cerberus analysis stage 1 and then after stage 1 is completed, you can then choose to run Cerberus Analysis stage 2.

By default, you must be a *Case Manager* to run Cerberus analysis.

To run a Cerberus Analysis

1. Do one of the following:

When creating a new case	In the *Case Manager*, in the *New Case Options* dialog, click **Detailed Options**. Select *Evidence Processing*, then click **Cerberus Analysis**.
If working an existing case	in the *Examiner*, go to *Evidence* > *Additional Analysis*. In the *Additional Analysis* dialog, under the section *Indexing* / *Tools*, click **Cerberus Analysis**.

2. Next to *Cerberus Analysis*, click **Cerberus Options**.
3. In the *Cerberus Analysis dialog*, you can define the weight assigned to each Cerberus stage 1 score. These Stage 1 scores are designed to identify and score specific malware properties and traits. The user-defined weights can be saved per case as well as globally in the Evidence Processing templates.
4. In the *Cerberus Analysis dialog*, you can choose the option *Perform Cerberus Analysis stage 2 if stage 1 threshold is greater than n.* This option lets you choose to automatically run stage 2 analysis after stage 1 analysis completes. Do one of the following:

To run stage 1 analysis only	Deselect the option to *Perform Cerberus Analysis stage 2 if stage 1 threshold is greater than,* then only Cerberus Analysis stage 1 is run.
To run both stage 1 and stage 2 analysis	Select the option to *Perform Cerberus Analysis stage 2 if stage 1 threshold is greater than n.* Specify a threshold for a minimum threat score against which you want to run the stage 2 analysis. If a file's threat score is higher than the threshold value that you set, then stage 2 is run.If a file's threat score is lower than the threshold value, then stage 2 analysis is not run. By default, the threshold automatically runs stage 2 analysis against files with a threat score greater than +20.

5. Click **OK**.
6. In the *Additional Analysis* dialog, click **OK**.

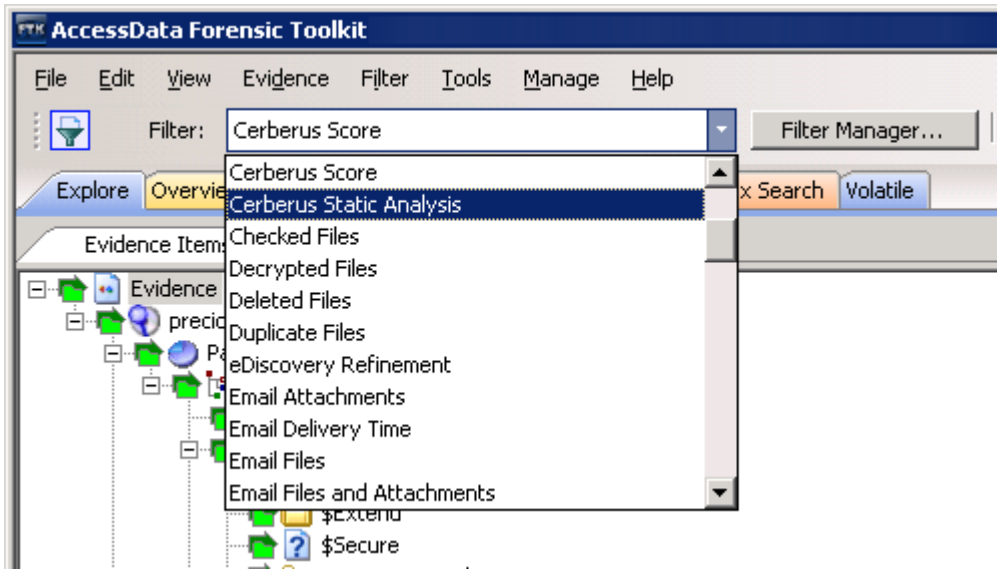
About Reviewing Results of Cerberus

You can use the *Examiner* to locate executable binaries that have had Cerberus analysis run against them. For executable binaries to have a Cerberus Score, a Case Administrator must first run a Cerberus Analysis.

The *Examiner* includes the following Cerberus filters that let you display only files that have had Cerberus run against them.

- *Cerberus Score*: Lets you limit the results that are displayed in the File List pane to only files that have had Cerberus Stage 1 analysis run against them.
- *Cerberus Static Analysis*: Lets you limit the results that are displayed in the File List pane to only files that have had both Cerberus Stage 1 analysis and Cerberus Stage 2 analysis.

Cerberus Filter View



Cerberus Columns

In the *File List* pane, there are Cerberus columns that display Cerberus results data.

See About Cerberus Stage 1 Threat Analysis on page 218.

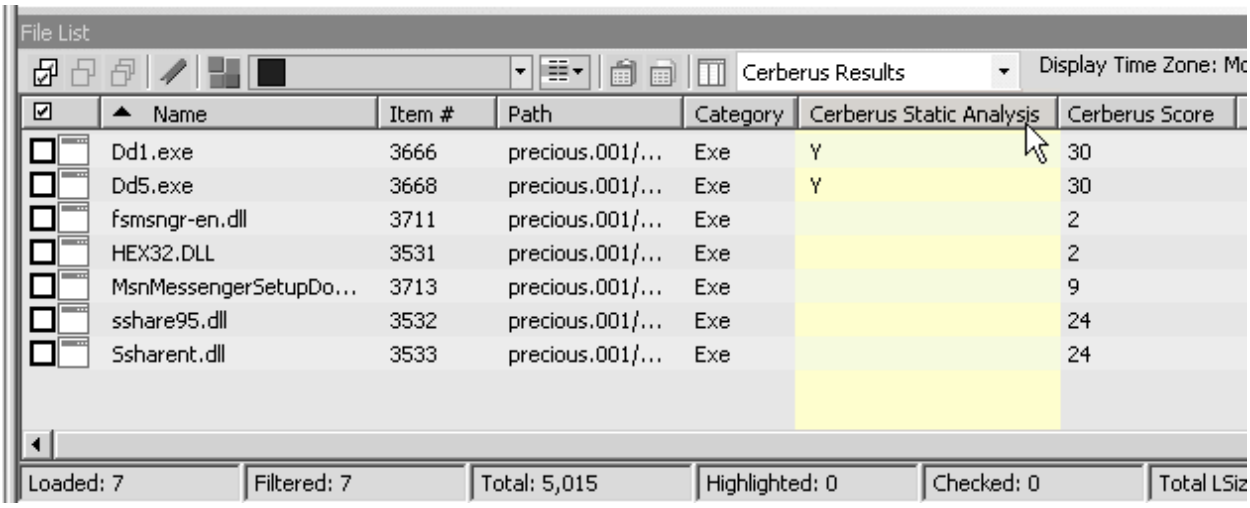
The data that the Cerberus filter uses to render the information is also available in columns in the *Item List*. These columns can be sorted and filtered.

There is a Column template that is pre-configured with columns for each of the Cerberus Threat Score Attributes.

See Icons of the File List Tool Bar on page 271.

You can you sort the list of files to see if they have had Cerberus Stage two Static Analysis run, see their threat score, or to see if they have attributes from a Cerberus stage 1 analysis.

Cerberus Columns


File List
Cerberus Results
Display Time Zone: Mo
Name
Item #
Path
Category
Cerberus Static Analysis
Cerberus Score
Dd1.exe 3666 precious.001/... Exe Y 30
Dd5.exe 3668 precious.001/... Exe Y 30
fsmsngr-en.dll 3711 precious.001/... Exe 2
HEX32.DLL 3531 precious.001/... Exe 2
MsnMessengerSetupDo... 3713 precious.001/... Exe 9
sshare95.dll 3532 precious.001/... Exe 24
Ssharent.dll 3533 precious.001/... Exe 24
Loaded: 7
Filtered: 7
Total: 5,015
Highlighted: 0
Checked: 0
Total LSiz

Reviewing Results of Cerberus

To view files with a Cerberus score

1. In the *Examiner*, open the *Explore* tab.
2. In the *Evidence Items* pane, use *Quick Picks* to select the evidence.
3. In the *Filter* drop-down menu, select one of the following:
   - *Cerberus Score*: Lets you limit the results that are displayed in the File List pane to only files that have had Cerberus Stage 1 analysis run against them.
   - *Cerberus Static Analysis*: Lets you limit the results that are displayed in the File List pane to only files that have had both Cerberus Stage 1 analysis and Cerberus Stage 2 analysis.
4. In the *File List* pane, in the *Column Setting* drop-down, select **Cerberus Results**.

   The *File List* pane shows all files that have been analyzed by Cerberus. It displays columns for each attribute that Cerberus 1 analyzes. If a file contained an attribute, the column cell displays a *Y*. If the file did not contain an attribute, the column cell displays an *N*. You can sort the files by clicking on a column heading. You can sort the displayed results by clicking a column header.
5. To view more details about the file, select it in the *File List* pane.

   Additional details about the Cerberus analysis are displayed in the *File Content* viewer in the *Natural* tab.

Using Index Search with Cerberus

The results of Cerberus analysis can be indexed so that you can run a search for them. The indexed information is an un-tagged version of the Cerberus HTML report. It is appended to the end of the content that is displayed in the File Content Pane's Filtered view.

See also Searching Evidence with Index Search (page 352).

To search for a Cerberus result

1. In the *Examiner*, click **Evidence > Additional Analysis**.
2. In the *Search Indexes* section, select **k® Text Index**.
3. In the *Miscellaneous* section, select **Cerberus Analysis**.
4. Click **Cerberus Options**.
5. Enter a Cerberus stage 2 Threshold and click **OK**.
6. In the *Additional Analysis* dialog, click **OK**.
7. In the *Examiner* click the **Index Search** tab.
8. In the *Terms* field, enter a value from the Cerberus report to search for and click **Add**. For example "Uses Cryptography."
9. Click **Search Now**.
10. (Optional) In the *Indexed Search FIlter Option* dialog, you can apply a filter. For example *Cerberus Score*.
11. Click **OK**.
12. In the *Indexed Results* pane, you can select a search result. The search hit is highlighted and displayed in the *File Content* pane.

Exporting a Cerberus Report

You can export Cerberus results to an HTML file.

To export a Cerberus Report

1. In the *File List* pane, right click a file that has Cerberus results.
2. Click **Export**.
3. In the *Export* dialog, under *File Options*, select **Save HTML view (if available)**.
4. In the *Destination base path* field, browse to the location where you want to save the export.
5. Click **OK**.

Chapter 16

Using the Known File Filter (KFF)

This chapter explains how to configure and use KFF and has the following sections:

- See Process for Using KFF on page 241.
- See About the KFF Admin page on page 242.
- See Adding Hashes to the KFF Server on page 244.
- See Using KFF Groups to Organize Hash Sets on page 248.
- See Enabling a Case to Use KFF on page 251.
- See Reviewing KFF Results in the Examiner on page 253.
- See Exporting KFF Data on page 256.

Process for Using KFF

To use the KFF feature, you perform the following steps:

Process for using KFF

Step 1.	Install and configure the KFF Server. See Installing the KFF Server on page 263.
Step 2.	Add and manage KFF hashes on the KFF Server. See Adding Hashes to the KFF Server on page 244.
Step 3.	Add and manage KFF Groups to organize KFF Hash Sets. Using KFF Groups to Organize Hash Sets (page 248)
Step 4.	Enable KFF for a case. See Enabling a Case to Use KFF on page 251.
Step 5.	Review KFF results in the Examiner. See Reviewing KFF Results in the Examiner on page 253.
Step 6.	(Optional) Re-process the KFF data using different hashes. See Re-Processing KFF Using Additional Analysis on page 255.
Step 7.	(Optional) Archive or export KFF data to share with other KFF Servers. See Exporting KFF Data on page 256.

About the KFF Admin page

You use the *KFF Admin* page to configure KFF Data by doing the following:

- Import Hashes
- Manually manage Hash Sets
- Create and manage KFF Groups
- Export KFF data

To open the KFF Admin page

❖ From the *Case Manager* or the *Examiner*, click **Manage** > **KFF..**.
The *KFF Admin* page opens.

If the *Configure KFF* dialog appears instead, check the following:

- The KFF Server is installed.
  See Installing the KFF Server on page 263.
- The application has been configured for the KFF Server.
  See Configuring the Location of the KFF Server on page 265.
- The KFF Service is running.
  In the Windows Services manager, make sure that the *AccessData Elasticsearch* service is started.

Elements of the KFF Admin page

Pane	Element	Description
Groups pane		Lets you create and manage KFF groups. See Using KFF Groups to Organize Hash Sets on page 248.
	New	Lets you create a KFF Group. See Creating a KFF Group on page 249.
	Edit	Lets you edit a KFF Group. See Managing KFF Groups on page 249.
	Delete	Lets you delete a KFF Group. See Managing KFF Groups on page 249.
	Export	You can share KFF hashes by exporting KFF groups. See Exporting KFF Data on page 256.
Hash Sets Pane		Displays the sets that you have imported or created. For example, if you import the NSRL KFF library, those sets are displayed here. Once you select a KFF Group in the Groups pane, only the Hash Sets and Groups that are in that selected group are listed.

Elements of the KFF Admin page

Pane	Element	Description
	Edit	Lets you edit the hashes in a custom Hash Set. See Using KFF Groups to Organize Hash Sets on page 248.
Import		Lets you import KFF data. See Importing KFF Data on page 244.
Archive Server		Lets you archive all of the custom KFF Groups and Hash Sets stored in this KFF Server. See Enabling a Case to Use KFF on page 251.

Adding Hashes to the KFF Server

You must add the hashes of the files that you want to compare against your evidence data. When adding hashes to the KFF Server, you add them in KFF Hash Sets.

You can use the following methods to add hashes to the KFF Library:

Migrate legacy KFF Server data	You can migrate legacy KFF data that is in a KFF Server in applications versions 5.5 and earlier. See Migrating Legacy KFF Data on page 266.
Import hashes	You can import previously configured KFF hashes, for example, from .CSV, .HDB, .HKE, or .HASH files. See Importing KFF Data on page 244.
Manually create and manage Hash Sets	You can manually add hashes to a Hash Set. See Manually Managing Hashes in a Hash Set on page 246.
Add hashes from files in your case	You can add hashes from files in your case. See Adding Hashes From Files in Cases on page 247.

Importing KFF Data

Before Importing KFF Data

To understand the methods and formats for importing KFF data, first see About Importing KFF Data (page 268).

This chapter explains how to import KFF data using the KFF Admin page.

Importing KFF Hashes

You can import KFF data from the following:

- KFF export files, such as CSV, TSV, HDB, HKE, KFF, HASH
- KFF binary files
  Warning: Importing KFF binary files will replace your existing KFF data.
  See About CSV and Binary Formats on page 275.
  It is recommended that you use the external *KFF Import Utility* to import KFF binary files.
  See Using the KFF Import Utility on page 269.

When importing KFF data, you must enter values for the following fields:

- Name
- Source Vendor
- Version
- Package

While the values are required, you can enter whatever values you may want to use to help you organize your hashes.

To import KFF hashes from files

1. Open the *Case Manager* or the *Examiner*.
2. Click **Manage** > **KFF**.
3. In *KFF Admin*, click **Import**.
4. Click **Add File**.
5. Set the Status: *Alert* or *Ignore*.
6. To browse to a file, for the *Path*, click **...**
7. Browse to the path of the file.
8. Use the file type selector to view the types of files that you are looking for (.CSV, HKE, KFF, etc.)
9. Select a file.
10. Click **Open**.
11. Enter information for the hash set:
12. Click **OK**.
13. (Optional) Add other files that you want to import.
14. Click **Import**.

To import KFF binary files

Warning: This process may replace your existing KFF data.

See About the KFF Binary Format on page 275.

1. Open the *Case Manager* or the *Examiner*.
2. Click **Manage** > **KFF**.
3. Click **Import**.
4. Click **Add File**.
5. Set the Status: *Alert* or *Ignore*.
6. Select *Import Entire Directory*.
7. To browse to a folder, for the *Path*, click **...**
8. Browse to the path of the source folder of the binary files (specifically the `Export.xml` file).
9. Click **Open**.
10. Enter information for the hash set:
11. After you have selected a file and added the information, click **OK**.
12. (Optional) Modify the import list by adding or removing files.
13. Click **Import**.

Manually Managing Hashes in a Hash Set

You can manually add, edit, and delete hash values within a custom hash set.

Note: You cannot manually add, edit, and delete hash values that were imported from NSRL, NDIC HashKeeper, and DHS libraries.

Searching For, Viewing, and Managing Hashes in a Hash Set

Due to the large number of hashes that may be in a Hash Set, a list of hashes is not displayed. (However, you can export a KFF Group that contains the Hash Set and view the hashes in the export file.)

You can use the KFF Hash Finder to search for hash values within a hash set. You search by entering a complete hash value. You can only search for one hash within one hash set at a time.

To search for and manage hashes in a hash set

1. Click **Manage > KFF**.
2. Select a Hash Set.
3. Click **Edit**.
4. To search for a hash, do the following:
   4a. In the *Hash* field, enter the complete hash value that you want to search for.
   4b. Click **Search**.
5. To manually add a hash to a hash set, do the following:
   5a. In the *Hash* field, enter the complete hash value that you want to add.
   5b. Click **Search** to verify if the hash already exists.
   5c. If the hash was not found, click **Add**.
   5d. Select the status of the hash:
      - Alert
      - Ignore
      - None
   5e. Enter the File Name of the file for the hash.
   5f. (Optional) Enter other information about the hash.
   5g. Click **Save**.
6. To manually edit a hash in a hash set, do the following:
   6a. In the *Hash* field, enter the complete hash value that you want to edit.
   6b. Click **Search** to verify that the hash already exists.
   6c. If the hash was found, click **Edit**.
   6d. Edit any settings and click **Save**.
7. To manually delete a hash from a hash set, do the following:
   7a. In the *Hash* field, enter the complete hash value that you want to delete.
   7b. Click **Search** to verify that the hash already exists.
   7c. If the hash was found, click **Delete**.
8. Click **Done**.

Adding Hashes From Files in Cases

You may identify files that in exist in a case as files that you want to add to your KFF hashes. For example, you may find a graphics file that you want to either alert for or ignore in this or other cases. Using *Examiner*, you can select files, export their file information to CSV, and then Import them as new KFF Hash Sets.

To add hashes from files in a case

1. Open a case in the Examiner.
2. Check one or more files that you want to have an Alert status for. (Only do similar statuses at a time.)
3. Export the file information you want to add hashes for by doing the following:
   3a. Click **File** > **Export File List Info**.
   3b. Browse to a folder and provide a name, such Files_for_KFF_Alerts.
   3c. Select a CSV format.
   3d. Choose *All checked*.
   3e. Click **Save.**
   3f. (Optional) Repeat the export for files that you want to have an Ignore status for.
4. Import one or more exported File List Info CSV files by doing the following:
   4a. Click **Manage** > **KFF**.
   4b. Click **Import**.
   4c. On the *KFF Import Tool,* click **Add File**.
   4d. Select the status: *Alert* or *Ignore* for the hashes.
   4e. Click **...** to browse to the file that you exported with the File List Info.
   4f. Enter the Source Vendor, Version, and Package.
   4g. Click **OK**.
   4h. (Optional) Click **Add file** and repeat for other files.
   4i. Click **Import**.
5. Add the new Hash Sets to one or more KFF Groups.

Using KFF Groups to Organize Hash Sets

About KFF Groups

KFF groups are containers for one or more Hash Sets. When you create a group, you then add Hash Sets to the group. KFF Groups can also contain other KFF Groups.

When you enable KFF for a case, you select which KFF Group to use during processing.

Within a KFF group, you can manually edit custom Hash Sets.

About KFF Groups Status Override Settings

When you create a KFF Group, you can choose to use the default status of the Hash Set (*Alert* or Ignore) or override it. You do this by setting one of the following Status Override settings:

- *Alert* - All Hash Sets within the KFF Group will be set to *Alert* regardless of the status of the individual Hash Sets.
- *Ignore* - All Hash Sets within the KFF Group will be set to *Ignore* regardless of the status of the individual Hash Sets.
- No Override - All Hash Sets will maintain their default status.

For example, if you have a Hash Set with a status of *Alert*, if you set the KFF Group to No Override, then the default status of *Alert* is used. If you set the KFF Group with a status of *Ignore*, the Hash Set *Alert* status is overridden and *Ignore* is used.

As a result, use caution when setting the Status Override for a KFF Group.

About Nesting KFF Groups

KFF Groups can contain Hash Sets or they can contain other KFF Groups. When one KFF Group includes another KFF Group, it is called nesting.

The reason that you may want to nest KFF Groups is that you can use multiple KFF Groups when processing your data. When you enable KFF for a case, you can only select one KFF Group. By nesting, you can use multiple KFF Groups.

For example, you may have one KFF Group that contains Hash Sets with an *Alert* status. You may have a second KFF Group that contains Hash Sets with an *Ignore* status. When processing a case, you may want to use both of those KFF Groups. To accomplish this, you can create another KFF Group as a parent and then add the other two KFF Groups to it. When processing, you would select the parent KFF Group.

When nesting KFF Groups you must be mindful of the Status Override of the parent KFF Group. When nesting KFF Groups, the Status Override the highest KFF Group in the hierarchy is used. In most cases, you will want to set the parent KFF Group with a status of *None*. That way, the status of each child KFF Group (or their Hash Sets) is used. If you select an *Alert* or *Ignore* status for the parent KFF Group, then all child KFF Groups and their Hash Sets will use that status.

About the Default KFF Group

A *Default* KFF Group is automatically created, but by default, has no Hash Sets in it. You cannot rename or delete the Default KFF Group however, you can add and remove Hash Sets.

The purpose of the *Default* KFF Group is that you can add the Hash Sets that you most regularly use, and when you enable the processing of KFF data for a case, you can simply select the *Default* KFF Group.

See Enabling a Case to Use KFF on page 251.

If you install NSRL, NDIC HashKeeper, and DHS libraries, they are automatically added to the *Default* KFF Group. You can remove them from the *Default* KFF Group if you wish.

Creating a KFF Group

You create KFF groups to organize your Hash Sets. When you create a KFF Group, you add one or more Hash Sets to it. You can later edit the KFF Group to add or remove Hash Sets.

To create and configure a KFF group

1. Open the *Case Manager* or the *Examiner*.
2. Click **Manage** > **KFF**.
3. In the *Groups* pane, click **New**.
4. Enter a *Name*.
5. Set the *Status Override*.
   See About KFF Groups Status Override Settings on page 248.
6. In the *Available Hash Sets* pane, select any hash sets to include in the KFF Group and click **<<** .
7. To nest another KFF Group within it, in the *Available Groups* pane, select any child KFF Groups and click **<<** .
8. Click **OK**.

Viewing the Contents of a KFF Group

In KFF Admin, you can select a KFF Group and in the right *Hash Sets* pane, view the Hash Sets and child KFF Groups that are contained in that KFF Group.

Managing KFF Groups

You can edit KFF Groups and do the following:

- Rename the group
- Change the Override Status
- Add or remove Hash Sets and KFF Groups

You can also do the following:

- Delete the group
- Export the group
  See Exporting KFF Data on page 256.

To manage a KFF Group

1. Open the *Case Manager* or the *Examiner*.
2. Click **Manage** > **KFF**.
3. Select a group or right-click a KFF Group.
4. Do one of the following:
   - Click **Edit**.
   - Click **Delete**.
   - Click **Export**.

Enabling a Case to Use KFF

About Enabling and Configuring KFF

To use KFF in a case, you do the following when you either create a case, add evidence to a case, or run *Additional Analysis*:

Process for enabling and configuring KFF

1. (Optional) Create a new case or add evidence to a case.	You can enable KFF when you create a case or add evidence to a case. You can also enable KFF for an existing case using Additional Analysis. See Re-Processing KFF Using Additional Analysis on page 255.
2. Configure how to process KFF Ignorable files	When you create a case or or add evidence to a case, you can choose how to process KFF Ignorable files: ● Exclude KFF Ignorable Files - By default, KFF will not include Ignorable files in the processed evidence. They will not be visible in the Examiner nor will they be in any file counts. ● Enable *Include KFF Ignorable Files* - You can enable a processing option to include KFF Ignorable files. Any files that are KFF Ignorable will be included and visible in the project. However, Ignorable files can be hidden using filters. See Enabling and Configuring KFF on page 251. See Using KFF Filters on page 254. When you process KFF using *Additional Analysis*, KFF Ignorable files are still included in the case's evidence files.
3. Enable KFF	Enable the *KFF* processing option. See Enabling and Configuring KFF on page 251.
4. Select a KFF Group	When you enable KFF, you select one KFF group to use. You can select an existing group or create a new group. A KFF Group can include other KFF Groups. You can select a parent KFF Group that contains other groups with the sets that you want to use See Using KFF Groups to Organize Hash Sets on page 248.

Enabling and Configuring KFF

To enable and configure KFF for a new case or new evidence

1. Create a new case or add evidence to a case and open the Evidence Processing options.
   See Evidence Processing Options on page 90.
   (In an existing case, open the *Additional Analysis* page.)
   See Using Additional Analysis on page 141.
   See Re-Processing KFF Using Additional Analysis on page 255.
2. Choose whether or not to include KFF Ignorable files.
   By default, KFF Ignorable files will not be included.
   To include KFF Ignorable files, do the following:
   2a. In the *Detailed Options* dialog, click the **Evidence Refinement (Advanced)** tab.
   2b. Select *Include KFF Ignorable Files*.

2c. Click the **Evidence Processing** tab.

3. In the *Evidence Processing* options, select *KFF*.
4. Do one of the following to select a KFF Group:
   - In the *KFF* drop-down menu, select and existing KFF Group that you want to use.
   - Click ... to open KFF Admin and configure a KFF Group to use and then select it.

   See About KFF Groups on page 248.

   You can use a KFF Group that you created or use the Default group.

   See About the Default KFF Group on page 249.
5. Configure any other processing options.
6. Click **OK**.

Reviewing KFF Results in the Examiner

You can view the KFF results in the Examiner. You can use the following tools to view KFF results:

- KFF Information in Columns
- KFF Filters
- KFF file status in the *Overview* tab.

About KFF Data Shown in the Item List

Depending on the KFF configuration options, you can identify and view files based on their KFF status and group.

Note: KFF Ignorable files will not be displayed in the File List unless you enabled the *Include KFF Ignorable Files* processing option.
See Enabling a Case to Use KFF on page 251.

There are three possible KFF statuses in the Examiner:

- *Alert* - Files that matched hashes in the template with an Alert status
- *Ignore* - Files that matched hashes in the template with an Ignore status (not shown in the *Item List* by default)
  See About Enabling and Configuring KFF on page 251.
- Unknown - Files that did not match hashes in the template (designated by a blank KFF Status)

Using the KFF Information Columns

You can add the following columns to display KFF data about each file in the File List.

KFF Columns

Column	Description
KFF Status	Displays the status of the file as it pertains to KFF. The three status options are *Alert, Ignore*, or Unknown (blank).
KFF Group	Displays the name of the KFF Group that has the matched hash.
Not KFF Ignore...	Displays a True status it if is not a KFF Ignorable file or a False status if it is a KFF Ignorable file.

Using KFF Filters

You can use filters to filter your evidence based on KFF data. You can use the Filter Manager to build a Compound filters.

To use the KFF Filters

1. In the *Examiner*, click the *Filter* drop-down menu.
2. Select one of the KFF Filters:
   - *KFF Alert Files* - Shows all files with an Alert status.
   - *KFF Ignore Files* - Shows all files with a KFF Ignore status.
     KFF Ignorable files will not be displayed unless you enabled the *Include KFF Ignorable Files* processing option.
     See Enabling a Case to Use KFF on page 251.
   - *No KFF Ignore Files* - Shows all files except those with a KFF Ignore status.

Using the Overview Tab

You can use the File Status nodes in the *Overview* tab to filter your evidence based on KFF data.

To use the Overview tab to filter KFF status

1. In the *Examiner*, click the **Overview** tab.
2. Expand *File Status*.
3. Click one of the following KFF nodes:
   - *KFF Alert Files* - Shows all files with an Alert status.
   - *KFF Ignorable Files* - Shows all files with a KFF Ignore status.
     KFF Ignorable files will not be displayed unless you enabled the *Include KFF Ignorable Files* processing option.
     See Enabling a Case to Use KFF on page 251.

Re-Processing KFF Using Additional Analysis

You can process an existing case with KFF using Additional Analysis in the following situations:

- After you have processed a case with KFF enabled, you can re-process your data using an updated or different KFF Group. This is useful in re-examining a project after adding or editing hash sets.

  See Adding Hashes From Files in Cases on page 247.

- Enabling KFF for a case that was not previously processed using KFF.

To re-process a case using KFF

1. In the *Examiner*, click **Evidence** > **Additional Analysis**.
2. Enable *KFF*.
3. Do one of the following:
   - In the the drop-down menu, select a KFF Group.
   - Configure a KFF Group by clicking the **...**.
4. You can either process files new files in the case or process files that have been processed previously against KFF.

   Mark **Recheck previously processed items** if you want to processes all existing files with the KFF Group that you have selected.
5. Click **OK**.
6. Review the KFF results.

   See Reviewing KFF Results in the Examiner on page 253.

Exporting KFF Data

About Exporting KFF Data

You can share KFF Hash Sets and KFF Groups with other KFF Servers by exporting KFF data on one KFF Server and importing it on another. You can also use export as a way of archiving your KFF data.

You can export data in one of the following ways:

- Exporting KFF Groups - This exports the selected KFF Groups with any included sub-groups and any included Hash Sets and hashes to a CSV file.
- Archiving the KFF Server's Data - This exports all the KFF data except NSRL, NIST, and DHC data in a binary format.

See About CSV and Binary Formats on page 275.

Exporting KFF Groups

You can share KFF hashes by exporting one or more KFF Groups. Exports are saved in a CSV file.

To export a KFF group

1. Open the *Case Manager* or the *Examiner*.
2. Click **Manage** > **KFF**.
3. Select one or more groups.
4. Click **Export**.
5. Select the location to which you want to save the exported CSV file.
6. Enter a name for the exported file.
7. Click **Save**.

Archiving the KFF Server's Data

You can archive all of the KFF Groups and custom Hash Sets stored in a KFF Server. This can be useful in backing up your KFF data or sharing data across other KFF Servers.

This archive does *not* include data that was imported from NSRL, NDIC HashKeeper, and DHS libraries.

The data is saved in either a CSV file or a binary format.

To archive a KFF Server

1. Open the *Case Manager* or the *Examiner*.
2. Click **Manage** > **KFF**.
3. In the Archive Server section, select *CSV file* or *Binary*.
4. Click **Archive Server...**
5. Select the location to which you want to save the export.
6. (CSV format only) Enter a name for the export.
7. Click **Save**.

Chapter 17

Getting Started with KFF (Known File Filter)

This document contains the following information about understanding and getting started using KFF (Known File Filter).

- About KFF (page 257)
- About the KFF Server and Geolocation (page 262)
- Installing the KFF Server (page 263)
- Configuring the Location of the KFF Server (page 265)
- Migrating Legacy KFF Data (page 266)
- Importing KFF Data (page 268)
- About CSV and Binary Formats (page 275)
- Installing KFF Updates (page 279)
- Uninstalling KFF (page 278)
- KFF Library Reference Information (page 280)
- What has Changed in Version 5.6 (page 285)

Important: AccessData applications versions 5.6, 6.0, and later use a new KFF architecture. If you are using one of the following applications version 5.6 or later, you must install and implement the new KFF architecture:

- FTK-based products (FTK, FTK Pro, AD Lab, AD Enterprise)
- eDiscovery

See What has Changed in Version 5.6 on page 285.

About KFF

KFF (Known File Filter) is a utility that compares the file hash values of known files against the files in your project. The known files that you compare against may be the following:

- Files that you want to ignore, such as operating system files
- Files that you want to be alerted about, such as malware or other contraband files

The hash values of files, such as MD5, SHA-1, etc., are based on the file's content, not on the file name or extension. The helps you identify files even if they are renamed.

Using KFF during your analysis can provide the following benefits:

- Immediately identify and ignore 40-70% of files irrelevant to the project.
- Immediately identify known contraband files.

Introduction to the KFF Architecture

There are two distinct components of the KFF architecture:

- KFF Data - The KFF data are the hashes of the known files that are compared against the files in your project. The KFF data is organized in KFF Hash Sets and KFF Groups. The KFF data can be comprised of hashes obtained from pre-configured libraries (such as NSRL) or custom hashes that you configure yourself.

  See Components of KFF Data on page 258.
- KFF Server - The KFF Server is the component that is used to store and process the KFF data against your evidence. The KFF Server uses the AccessData Elasticsearch Windows Service. After you install the KFF Server, you import your KFF data into it.

Note: The KFF database is no longer stored in the shared evidence database or on the file system in EDB format.

Components of KFF Data

Item	Description
Hash	The unique MD5 or SHA-1 hash value of a file. This is the value that is compared between known files and the files in your project.
Hash Set	A collection of hashes that are related somehow. The hash set has an ID, status, name, vendor, package, and version. In most cases, a set corresponds to a collection of hashes from a single source that have the same status.
Group	KFF Groups are containers that are used for managing the Hash Sets that are used in a project. KFF Groups can contains Hash Sets as well as other groups. Projects can only use a single KFF Group. However, when configuring your project you can select a single KFF Group which can contains nested groups.
Status	The specified status of a hash set of the known files which can be either Ignore or Alert. When a file in a project matches a known file, this is the reported status of the file in the project.
Library	A pre-defined collection of hashes that you can import into the KFF Serve. There are three pre-defined libraries: ● NSRL ● NDIC HashKeeper ● DHS See About Pre-defined KFF Hash Libraries on page 260.

Item	Description
Index/Indices	When data is stored internally in the KFF Library, it is stored in multiple indexes or indices. The following indices can exist: ● NSRL index A dedicated index for the hashes imported from the NSRL library. ● NDIC index A dedicated index for the hashes imported from the NDIC library. ● DHC index A dedicated index for the hashes imported from the DHC library. ● KFF index A dedicated index for the hashes that you manually create or import from other sources, such as CSV. These indices are internal and you do not see them in the main application. The only place that you see some of them are in the KFF Import Tool. See Using the KFF Import Utility on page 269. The only time you need to be mindful of the indices is when you use the KFF binary format when you either export or import data. See About CSV and Binary Formats on page 275.

About the Organization of Hashes, Hash Sets, and KFF Groups

Hashes, such as MD5, SHA-1, etc., are based on the file's content, not on the file name or extension.

You can also import hashes into the KFF Server in **.CSV** format.

For FTK-based products, you can also import hashes into the KFF Server that are contained in **.TSV**, **.HKE**, **.HKE.TXT**, .HDI, .HDB, **.hash**, **.NSRL**, or **.KFF** file formats.

You can also manually add hashes.

Hashes are organized into Hash Sets. Hash Sets usually include hashes that have a common status, such as Alert or Ignore.

Hash Sets must be organized into to KFF Groups before they can be utilized in a project.

About Pre-defined KFF Hash Libraries

All of the pre-configured hash sets currently available for KFF come from three federal government agencies and are available in KFF libraries.

See About KFF Pre-Defined Hash Libraries on page 280.

You can use the following KFF libraries:

- NIST NSRL
  See About Importing the NIST NSRL Library on page 272.
- NDIC HashKeeper (Sept 2008)
  See Importing the NDIC Hashkeeper Library on page 273.
- DHS (Jan 2008)
  See Importing the DHS Library on page 274.

It is not required to use a pre-configured KFF library in order to use KFF. You can configure or import custom hash sets. See your application's *Admin Guide* for more information.

How KFF Works

The Known File Filter (KFF) is a body of MD5 and SHA1 hash values computed from electronic files. Some pre-defined data is gathered and cataloged by several US federal government agencies or you can configure you own. KFF is used to locate files residing within project evidence that have been previously encountered by other investigators or archivists. Identifying previously cataloged (known) files within a project can expedite its investigation.

When evidence is processed with the MD5 Hash (and/or SHA-1 Hash) and KFF options, a hash value for each file item within the evidence is computed, and that newly computed hash value is searched for within the KFF data. Every file item whose hash value is found in the KFF is considered to be a known file.

Note: If two hash sets in the same group have the same MD5 hash value, they must have the same metadata. If you change the metadata of one hash set, all hash sets in the group with the same MD5 hash file will be updated to the same metadata.

The KFF data is organized into Groups and stored in the KFF Server. The KFF Server service performs lookup functions.

Status Values

In order to accelerate an investigation, each known file can labeled as either Alert or Ignore, meaning that the file is likely to be forensically interesting (Alert) or uninteresting (Ignore). Other files have a status of Unknown.

The Alert/Ignore designation can assist the investigator to hone in on files that are relevant, and avoid spending inordinate time on files that are not relevant. Known files are presented in the Overview Tab's File Status Container, under "KFF Alert files" and "KFF Ignorable."

Hash Sets

The hash values comprising the KFF are organized into hash sets. Each hash set has a name, a status, and a listing of hash values. Consider two examples. The hash set “ZZ00001 Suspected child porn” has a status of Alert and contains 12 hash values. The hash set “BitDefender Total Security 2008 9843” has a status of Ignore and contains 69 hash values. If, during the course of evidence processing, a file item’s hash value were found to belong to the “ZZ00001 Suspected child porn” set, then that file item would be presented in the KFF Alert files list. Likewise, if another file item’s hash value were found to belong to the “BitDefender Total Security 2008 9843” set, then that file would be presented in the KFF Ignorable list.

In order to determine whether any Alert file is truly relevant to a given project, and whether any Ignore file is truly irrelevant to a project, the investigator must understand the origins of the KFF’s hash sets, and the methods used to determine their Alert and Ignore status assignments.

You can install libraries of pre-defined hash sets or you can import custom hash sets. The pre-defined hash sets contain a body of MD5 and SHA1 hash values computed from electronic files that are gathered and cataloged by several US federal government agencies.

See About KFF Pre-Defined Hash Libraries on page 280.

Higher Level Structure and Usage

Because hash set groups have the properties just described, and because custom hash sets and groups can be defined by the investigator, the KFF mechanism can be leveraged in creative ways. For example, the investigator may define a group of hash sets created from encryption software and another group of hash sets created from child pornography files and then apply only those groups while processing.

About the KFF Server and Geolocation

In order to use the Geolocation Visualization feature in various AccessData products, you must use the KFF architecture and do the following:

- Install the KFF Server.
  See Installing the KFF Server on page 263.
- Install the Geolocation (GeoIP) Data (this data provide location data for evidence)
  See Installing the Geolocation (GeoIP) Data on page 274.
  From time to time, there will be updates available for the GeoIP data.
  See Installing KFF Updates on page 279.

If you are upgrading to 5.6 or later from an application 5.5 or earlier, you must install the new KFF Server and the updated Geolocation data.

Installing the KFF Server

About Installing the KFF Server

In order to use KFF, you must first install and configure a KFF Server.

For product versions 5.6.x and 6.0.x and later, you install a KFF Server by installing the AccessData Elasticsearch Windows Service.

Where you install the KFF Server depends on the product you are using with KFF:

- For FTK and FTK Pro applications, the KFF Server must be installed on the same computer that runs the FTK Examiner application.
- For all other applications, such as eDiscovery, AD Lab, the KFF Server can be installed on either the same computer as the application or on a remote computer. For large environments, it is recommended that the KFF Server be installed on a dedicated computer.

Once the KFF components are installed, they will be accessible via the *Windows Start Menu*, as well as through FTK in the *Manage* menu.

Note: KFF components will only be available in the *Windows Start Menu* on the computer where they are physically installed.

After installing the KFF Server, you configure the application with the location of the KFF Server.

See Configuring the Location of the KFF Server on page 265.

About KFF Server Versions

The KFF Server (AccessData Elasticsearch Windows Service) may be updated from time to time. It is best to use the latest version.

AccessData Elasticsearch Windows Service	Released	Installation Instructions

Version 1.3.2.x	• November 2014 with 5.6 versions of
	  ▪ FTK-based products
	  ▪ eDiscovery
	• November 2015 with 6.0 versions of
	  ▪ FTK-based products
	  ▪ eDiscovery
		See Installing the KFF Server Service on page 264.

For applications 5.5 and earlier, the KFF Server component was version 1.2.7 and earlier.

About Upgrading from Earlier Versions

If you have used KFF with applications versions 5.5 and earlier, you can migrate your legacy KFF data to the new architecture.

See Migrating Legacy KFF Data on page 266.

Process for Installing KFF

The process for installing KFF is as follows:

1. Downloading the Latest KFF Installation Files (page 264)
2. Installing the KFF Server Service (page 264)
3. Configuring the KFF Server location:
   - Configuring the KFF Server Location on FTK-based Applications (page 265)
   - Configuring the KFF Server Location on eDiscovery (page 265)
4. (Optional) Upgrading or importing KFF data.
   - See Migrating Legacy KFF Data on page 266.
   - About Importing KFF Data (page 268)
   - Importing Pre-defined KFF Data Libraries (page 271)
   - Installing the Geolocation (GeoIP) Data (page 274)

Downloading the Latest KFF Installation Files

You can download ISO files which has the latest KFF files. Files may be updated from time to time.

To download the latest KFF Installation Files

1. Go to the AccessData Current Releases - Digital Forensics product download page.
   You can also download the file from the FTK or AD Lab product download pages.
2. Click **Known File Filter (KFF) Compatible with 5.6 and above**.
3. Do one of the following:
   - To download the KFF Server files, utilities, and NSRL data, click **KFF for all 6.0 products**.
   - To download the DHS library, click **KFF DHS**.
   - To download the NDIC library, click **KFF NDIC**.
4. Click **Download Now.**

Installing the KFF Server Service

The KFF Server Service is install by installing the AccessData Elasticsearch Windows Service

For instructions on installing the AccessData Elasticsearch Windows Service, see Installing the Elasticsearch Service (page 512).

Configuring the Location of the KFF Server

After installing the KFF Server, on the computer running the application, such as eDiscovery, FTK, or AD Lab, you configure the location of the KFF Server.

Do one of the following:

- Configuring the KFF Server Location on FTK-based Applications (page 265)
- Configuring the KFF Server Location on eDiscovery (page 265)

Configuring the KFF Server Location on FTK-based Applications

Before using KFF with FTK, FTK Pro, Lab, or Enterprise, with KFF, you must configure the location of the KFF Server.

Important: To configure KFF, you must be logged in with Admin privileges.

To view or edit KFF configuration settings

1. In the *Case Manager*, click **Tools > Preferences > Configure KFF**.
2. You can set or view the address of the KFF Server.
   - If you installed the KFF Server on the same computer as the application, this value will be localhost.
   - If you installed the KFF Server on a different computer, identify the KFF server.
3. Click **Test** to validate communication with the KFF Server.
4. Click **Save**.
5. Click **OK**.

Configuring the KFF Server Location on eDiscovery

When using the KFF Server with eDiscovery, two configuration files must point to the KFF Server location.

If one of the following is true, these setting are configured automatically during the KFF Server installation.

- Your eDiscovery installation is on a single server
- Your eDiscovery installation is on multiple servers, and you install the KFF Server on the same server that is running WorkManager

If needed, you can verify the settings.

However, if one of the following is true, you must manually specify the location of the KFF Server:

- If you change the location of your KFF Server
- Your eDiscovery installation is on multiple servers, and you install the KFF Server on a different server than is running WorkManager

Manually Configuring the KFF Server Location

1. Configure `AdgWindowsServiceHost.exe.config`:
   1a. On the computer running the work manger service, go to `C:\Program Files\AccessData\Common\FTK Business Services`.
   1b. Open `AdgWindowsServiceHost.exe.config`.
   1c. Modify the line `<add key="KffElasticSearchUrl" value="http://localhost:9200" />`.

1d. Change *localhost* to be the location of your KFF server (you can use hostname or IP).

1e. Save and close file.

1f. Restart the AccessData Business Services Common service.

2. Configure **Infrastructure.WorkExecutionServices.Host.exe.config**:

2a. On the computer running the work manger service, go to **C:\Program Files\AccessData\eDiscovery\WorkManager**.

2b. Open **Infrastructure.WorkExecutionServices.Host.exe.config**.

2c. Modify the line **<add key="KffElasticSearchUrl" value="http://localhost:9200" />**.

2d. Change *localhost* to be the location of your KFF server (you can use hostname or IP).

2e. Save and close file.

2f. Restart the AccessData Work Manager service.

Migrating Legacy KFF Data

If you have used KFF with applications versions 5.5 and earlier, you can migrate that data from the legacy KFF Server to the new KFF Server architecture.

Important: Applications version 5.6 and later can only use the new KFF architecture that was introduced in 5.6. If you want to use KFF data from previous versions, you must migrate the data.

Important: If you have NSRL, NDIC, or DHS data in your legacy data, those sets will not be migrated. You must re-import them using the 5.6 versions or later of those libraries. Only legacy custom KFF data will be migrated.

Legacy KFF data is migrated to KFF Groups and Hash Sets on the new KFF Server.

Because KFF Templates are no longer used, they will be migrated as KFF Groups, and the groups that were under the template will be added as sub-groups.

You migrate data using the KFF Migration Tool. To use the KFF Migration Tool, you identify the following:

- The Storage Directory folder where the legacy KFF data is located.
  This was folder was configured using the KFF Server Configuration utility when you installed the legacy KFF Server. If needed, you can use this utility to view the KFF Storage Directory. The default location of the KFF_Config.exe file is Program Files\AccessData\KFF.
- The URL of the new KFF Server (the computer running the AccessData Elastic Search Windows Service)
  This is populated automatically if the new KFF Server has been installed.

To install the KFF Migration Tool

1. On the computer where you have installed the KFF Server, access the KFF Installation disc, and run the **autorun.exe**.
2. Click the *64 bit* or *32 bit* **Install KFF Migration Utility**.
3. Complete the installation wizard.

To migrate legacy KFF data

1. On the legacy KFF Server, you must stop the KFF Service.
   You can stop the service manually or use the legacy KFF Config.exe utility.
2. On the new KFF Server, launch the KFF Migration Tool.
3. Enter the directory of the legacy KFF data.

4. The URL of Elasticsearch should be listed.
5. Click **Start**.
6. When completed, review the summary data.

Importing KFF Data

About Importing KFF Data

You can import hashes and KFF Groups that have been previous configured.

You can import KFF data in one of the following formats:

KFF Data sources that you can import

Source	Description
Pre-configured KFF libraries	You can import KFF data from the following pre-configured libraries ● NIST NSRL ● NDIC HashKeeper ● DHS To import KFF libraries, it is recommended that you use the KFF Import Utility. See Using the KFF Import Utility on page 269. See Importing Pre-defined KFF Data Libraries on page 271. See KFF Library Reference Information on page 280.
Custom Hash Sets and KFF Groups	You can import custom hashes from CSV files. See About the CSV Format on page 275. For FTK-based products, you can also import custom hashes from the following file types: ● Delimited files (CSV or TSV) ● Hash Database files (HDB) ● Hashkeeper files (HKE) ● FTK Exported KFF files (KFF) ● FTK Supported XML files (XML) ● FTK Exported Hash files (HASH) To import these kinds of files, use the KFF Import feature in your application. See *Using the Known File Feature* chapter.
KFF binary files	You can import KFF data that was exported in a KFF binary format, such as an archive of a KFF Server. See About CSV and Binary Formats on page 275. When you import a KFF binary snapshot, you must be running the same version of the KFF Server as was used to create the binary export. To import KFF binary files, it is recommend that you use the KFF Import Utility. See Using the KFF Import Utility on page 269.

About KFF Data Import Tools

When you import KFF data, you can use one of two tools:

KFF Data Import Tools

The application's Import feature	The KFF management feature in the application lets you import both .CSV and KFF Binary formats. Use the application to import .CSV files. See *Using the Known File Feature* chapter. Even though you can import KFF binary files using the application, it is recommend that you use the KFF Import Utility.
KFF Import Utility	It is recommended that you use the KFF Import Utility to import KFF binary files. See Using the KFF Import Utility on page 269.

About Default Status Values

When you import KFF data, you configure a default status value of Alert or Ignore. When adding Hash Sets to KFF Groups, you can configure the KFF Groups to use the default status values of the Hash Set or you can configure the KFF Group with a status that will override the default Hash Set values.

See Components of KFF Data on page 258.

About Duplicate Hashes

If multiple Hash Set files containing the same Hash identifier are imported into a single KFF Group, the group keeps the last Hash Set's metadata information, overwriting the previous Hash Sets' metadata. This only happens within an individual group and not across multiple groups.

Using the KFF Import Utility

About the KFF Import Utility

Due to the large size of some KFF data, a stand-alone KFF Import utility is available to use to import the data. This KFF Import utility can import large amounts of data faster then using the import feature in the application.

It is recommend that you install and use the KFF Import utility to import the following:

- NSRL, DHC, and NIST libraries
- An archive of a KFF Server that was exported in the binary format

After importing NSRL, NDIC, or DHS libraries, these indexes are displayed in the *Currently Installed Sets* list.

See Components of KFF Data on page 258.

You can also use the KFF Import Utility to remove the NSRL, NDIC, or DHS indexes that you have imported.

An archive of a KFF Server, which is the exported *KFF Index*, is not shown in the list.

Installing the KFF Import Utility

You should use the KFF Import Utility to import some kinds of KFF data.

To install the KFF Import Utility

1. On the computer where you have installed the KFF Server, access the KFF Installation disc, and run the `autorun.exe`.
2. Click the *64 bit* or *32 bit* **Install KFF Import Utility**.
3. Complete the installation wizard.

Importing a KFF Server Archive Using the KFF Import Utility

You can import an archive of a KFF Server that you have exported using the binary format.

If you are importing a pre-defined KFF Library, see Importing Pre-defined KFF Data Libraries (page 271).

To import using the KFF Import Utility

1. On the KFF Server, open the KFF Import Utility.
2. To test the connection to the KFF Server's Elasticsearch service at the displayed URL, click **Connect**.
   If it connects correctly, no error is shown.
   If it is not able to connect, you will get the following error: Failed after retrying 10 times: 'HEAD accessdata_threat_indicies'.
3. To import, click **Import**.
4. Click **Browse**.
5. Browse to the folder that contains the KFF binary files.
   Specifically, select the folder that contains the Export.xml file.
6. Click **Start**.
7. Close the dialog.

Removing Pre-defined KFF Libraries Using the KFF Import Utility

You can remove a pre-defined KFF Library that you have previously imported.

You cannot see or remove existing custom KFF data (the *KFF Index*).

To remove pre-defined KFF Libraries

1. On the KFF Server, open the KFF Import Utility.
2. Select the library that you want to remove.
3. Click **Remove**.

Importing Pre-defined KFF Data Libraries

About Importing Pre-defined KFF Data Libraries

After you install the KFF Server, you can import pre-defined NIST NSRL, NDIC HashKeeper, and DHS data libraries.

See About Pre-defined KFF Hash Libraries on page 260.

In versions 5.5 and earlier, you installed these using an executable file. In versions 5.6 and later, you must import them. It is recommend that you use the KFF Import Utility.

After importing pre-defined KFF Libraries, you can remove them from the KFF Server.

See Removing Pre-defined KFF Libraries Using the KFF Import Utility on page 270.

See the following sections:

- About Importing the NIST NSRL Library (page 272)
- Importing the NDIC Hashkeeper Library (page 273)
- Importing the DHS Library (page 274)

About Importing the NIST NSRL Library

You can import the NSRL library into your KFF Server. During the import, two KFF Groups are created: NSRL_Alert and NSRL_Ignore. In FTK-based products, these two groups are automatically added to the Default KFF Group.

The NSRL libraries are updated from time to time. To import and maintain the NSRL data, you do the following:

Process for Importing and Maintaining the NIST NSRL Library

1. Import the complete NSRL library.	You must first install the most current complete NSRL library. You can later add updates to it. To access and import the complete NSRL library, see Importing the Complete NSRL Library (page 273)
2. Import updates to the library	When updates are made available, import the updates to bring the data up-to date. See Installing KFF Updates on page 279. **Important:** In order to use the NSRL updates, you must first import the complete library. When you install an NSRL update, you must keep the previous NSRL versions installed in order to maintain the complete set of NSRL data.

Available NRSL library files (new format)

NSRL Library Release	Released	Information
Complete library version 2.45 (source .ZIP file)	Nov 2014	For use only with applications version 5.6 and later. Contains the full NSRL library up through update 2.45. See Importing the Complete NSRL Library on page 273.

Available Legacy NRSL library files

Legacy NSRL Library Release	Released	Information
version 2.44 (.EXE file)	Nov 2013	For use with the legacy KFF Server that was used with applications versions 5.5 and earlier. Contains the full NSRL library up through update 2.44. Install this library first. **Note:** NSRL updates for the legacy KFF format will end in the 2nd quarter of 2015. From that time, NSRL updates will only be provided in the new format.

Importing the Complete NSRL Library

To add the NSRL library to your KFF Library, you import the data. You start by importing the full NSRL library. You can then import any updates as they are available.

See About Importing the NIST NSRL Library on page 272.

See Installing KFF Updates on page 279.

Important: The complete NSRL library data is contained in a large (3.4 GB) .ZIP file. When expanded, the data is about 18 GB. Make sure that your file system can support files of this size.

Important: Due to the large amount of NSRL data, it will take 3-4 hours to import the NSRL data using the KFF Import Utility. If you import from within an application, it will take even longer.

To install the NSRL complete library

1. Extract the NSRLSOURCE_2.45.ZIP file from the KFF Installation disc.
   See Downloading the Latest KFF Installation Files on page 264.
2. On the KFF Server, launch the *KFF Import Utility*.
   See Installing the KFF Import Utility on page 270.
3. Click **Import**.
4. Click **Browse**.
5. Browse to and select the NSRLSource_2.45 folder that contains the **NSRLFile.txt** file.
   (Make sure you are selecting the folder and not drilling into the folder to select an individual file. The import process will drill into the folder to get the proper files for you.)
6. Click **Select Folder**.
7. Click **Start**.
8. When the import is complete, click **OK**.
9. Close the *Import Utility* dialog and the NSRL library will be listed in the *Currently Installed Sets*.

Importing the NDIC Hashkeeper Library

You can import the Hashkeeper 9.08 library.

For application versions 5.6 and later, these files are stored in the KFF binary format.

To import the Hashkeeper library

1. Have access the NDIC source files by download the ZIP file from the web:
   See Downloading the Latest KFF Installation Files on page 264.
2. Extract the ZIP file.
3. On the KFF Server, launch the *KFF Import Utility*.
   See Installing the KFF Import Utility on page 270.
4. Click **Import**.
5. Click **Browse**.
6. Browse to and select the NDIC source folder that contains the **Export.xml** file.
   (Make sure you are selecting the folder and not drilling into the folder to select an individual file. The import process will drill into the folder to get the proper files for you.)
7. Click **Select Folder**.

8. Click **Start**.
9. When the import is complete, click **OK**.
10. Close the *Import Utility* dialog and the NDIC library will be listed in the *Currently Installed Sets*.

Importing the DHS Library

You can import the DHS 1.08 library.

For application versions 5.6 and later, these files are stored in the KFF binary format.

To import the DHS library

1. Have access the NDIC source files by download the ZIP file from the web:
   See Downloading the Latest KFF Installation Files on page 264.
2. Extract the ZIP file.
3. On the KFF Server, launch the *KFF Import Utility*.
   See Installing the KFF Import Utility on page 270.
4. Click **Import**.
5. Click **Browse**.
6. Browse to and select the DHS source folder that contains the **Export.xml** file.
   (Make sure you are selecting the folder and not drilling into the folder to select an individual file. The import process will drill into the folder to get the proper files for you.)
7. Click **Select Folder**.
8. Click **Start**.
9. When the import is complete, click **OK**.
10. Close the *Import Utility* dialog and the DHS library will be listed in the *Currently Installed Sets*.

Installing the Geolocation (GeoIP) Data

Geolocation (GeoIP) data is used for the Geolocation Visualization feature of several AccessData products.

See About the KFF Server and Geolocation on page 262.

You can also check for and install GeoIP data updates.

If you are upgrading to 5.6 or later from an application 5.5 or earlier, you must install the new KFF Server and the updated Geolocation data.

The Geolocation data that was used with versions 5.5 and earlier is version 1.0.1 or earlier.

The Geolocation data that is used with versions 5.6 and later is version 2014.10 or later.

To install the Geolocation IP Data

1. On the computer where you have installed the KFF Server, access the KFF Installation disc, and run the **autorun.exe**.
   See Downloading the Latest KFF Installation Files on page 264.
2. Click the *64 bit* or *32 bit* **Install Geolocation Data**.
3. Complete the installation wizard.

About CSV and Binary Formats

When you export and import KFF data, you can use one of two formats:

- CSV
- KFF Binary

About the CSV Format

When you use the .CSV format, you use a single .CSV file. The .CSV file contains the hashes that you import or export.

When you export to a CSV file, it contains the hashes as well as all of the information about any associated Hash Sets and KFF Groups. You can only use the CSV format when exporting individual Hash Sets and KFF Groups.

When you import using a CSV file, it can be a simple file containing only the hashes of files, or it can contain additional information about Hash Sets and KFF Groups.

However, CSV files will usually take a little longer to export and import.

To view the sample of a .CSV file that contains binaries and Hash Sets and KFF Groups, perform a CSV export and view the file in Excel.

You can also use the format of CSV files that were exported in previous versions.

To import .CSV files, use the application's KFF Import feature.

About the KFF Binary Format

When you use the KFF binary format, you use a set of files that are in an internal KFF Server (Elasticsearch) format that is referred to as a Snapshot. The binary format is essentially a snapshot of one of the indices contained in the KFF Server. You can only have one binary format snapshot for each index.

See Components of KFF Data on page 258.

The benefit of the binary format is that it is able to support larger amounts of data than the CSV format. For large data sets, the binary format will export and import faster than the CSV format.

For example, when you import the DHC or NDIC Hashkeeper libraries, they are imported from a KFF binary format.

If you export your custom Hash Sets or KFF Groups using the KFF binary format, everything in the *KFF Index* is included.

See About Choosing to Export in CSV or KFF Binary Format on page 276.

When exporting in a Binary format, you specify an existing parent folder and then the name of a new sub-folder for the binary data. The new sub-folder must not previously exist and will be created by the export process.

After export, the binary export folder contains the following:

- **Indices** sub-folder - The folder contains the exported KFF data
- **Export.xml** - This file is the only file that is not an Elasticsearch file and is created by the export feature and contains the KFF Group and Hash Set definitions for the index.

- **Index** - an index file generated by Elasticsearch
- **metadata-snaphot** file with the data and time it was created
- **snapshot-snaphot** file with the data and time it was created

Note: The binary format is dependent on the version of the KFF Server. When exporting and importing the binary format, the systems must be using the same version of the KFF Server.
When new versions of the KFF Server are released in the future, an upgrade process will also be provided.

About Choosing to Export in CSV or KFF Binary Format

When you export your own KFF data, you have the option of using either the CSV or the binary format. The results are different based on the format that you use:

CSV format	
Exporting in CSV format	When you export KFF data using the CSV format, you can export specific pieces of KFF data, such as one or more Hash Sets or one or more KFF Groups. The exported data is contained in one .CSV file. The benefits of the CSV format are that CSV files can be easily viewed and can be manually edited. They are also less dependent on the version of the KFF Server.
Importing from CSV format	When you import a CSV file, the data in the file is data is added to your existing KFF data that is in the *KFF Index*. See Components of KFF Data on page 258. For example, suppose you started by manually created four Hash Sets and one KFF Group. That would be the only contents in your *KFF Index*. Suppose you import a .CSV file that contains five hash sets and two KFF Groups. They will be added together for a total of nine Hash Sets and three KFF Groups. To import .CSV files, use the KFF Import feature in your application. See *Using the Known File Feature* chapter.
KFF binary format	
Exporting in KFF binary format	If you export your KFF data using the KFF binary format, all of the data that you have in the *KFF Index* will be exported together. You cannot use this format to export individual Hash Sets or KFF Groups. See Components of KFF Data on page 258. You will only want to use this format if you intend to export all of the data in the *KFF Index* and import it as a whole. This can be useful in making an archive of your KFF data or copying KFF data from one KFF Server to another. Because NSRL, NIST, and DHC data is contained in their own indexes, when you do an export using this format, those sets are not included. Only the data in the *KFF Index* is exported.

Importing KFF binary format	**IMPORTANT:** When you import a KFF binary format, it will import the complete index and will *replace* any data that is currently in that index on the KFF Server. For example, if you import the DHC library, and then later you import the DHC library again, the DHC index will be replaced with the new import. If you have a KFF binary format snapshot of custom KFF data (which would have come from a binary format export) it will replace all KFF data that already exists in your *KFF Index*. For example, suppose you manually created four Hash Sets and one KFF Group. Suppose you then import a binary format that has five hash sets and two KFF Groups. The binary format will be imported as a complete index and will replace the existing data. The result will be only be the imported five Hash Sets and two KFF libraries. When importing KFF binary files, it is recommend that you use the KFF Import Utility. See Installing the KFF Import Utility on page 270.

Uninstalling KFF

You can uninstall KFF application components independently of the KFF Data.

Main version	Description
Applications 5.6 and later	For applications version 5.6 and later, you uninstall the following components: ● *AccessData Elasticsearch Windows Service* (KFF Server) v1.2.7 and later Note: Elasticsearch is used by multiple features in various applications, use caution when uninstalling this service or the related data. ● *AccessData KFF Import Utility* (v5.6 and later) ● *AccessData KFF Migration Tool* (v1.0 and later) ● *AccessData Geo Location Data* (v2014.10 and later) Note: This component is not used by the KFF feature, but with the KFF Server for the geolocation visualization feature. The location of the KFF data is configured when the *AccessData Elasticsearch Windows Service* was installed. By default, it is located at C:\Program Files\AccessData\Elacticsearch\Data.
Applications 5.5 and earlier	For applications version 5.5 and earlier, you can uninstall the following components: ● KFF Server (v1.2.7 and earlier) Note: The KFF Server is also used by the geolocation visualization feature. ● AccessData Geo Location Data (1.0.1 and earlier) This component is not used by the KFF feature, but with the KFF Server for the geolocation visualization feature. The location of the KFF data was configured when the *KFF Server* was installed. You can view the location of the data by running the *KFF.Config.exe* on the KFF Server. If you are upgrading from 5.5 to 5.6, you can migrate your KFF data before uninstalling the KFF Server.

Installing KFF Updates

From time to time, AccessData will release updates to the KFF Server and the KFF data libraries.

Some of the KFF data updates may require you to update the version of the KFF Server.

To check for updates, do the following:

1. Go to the KFF product download page.
   See Downloading the Latest KFF Installation Files on page 264.
2. Check for updates.
   - See About KFF Server Versions on page 263.
   - See About Importing the NIST NSRL Library on page 272.
3. If there are updates, download them.
4. Install or import the updates.

KFF Library Reference Information

About KFF Pre-Defined Hash Libraries

This section includes a description of pre-defined hash collections that can be added as AccessData KFF data.

The following pre-defined libraries are currently available for KFF and come from one of three federal government agencies:

- NIST NSRL (The default library installed with KFF)
- NDIC HashKeeper (An optional library that can be downloaded from the AccessData Downloads page)
- DHS (An optional library that can be downloaded from the AccessData Downloads page)

Note: Because KFF is now multi-sourced, it is no longer maintained in HashKeeper format. Therefore, you cannot modify KFF data in the HashKeeper program. However, the HashKeeper format continues to be compatible with the AccessData KFF data.

Use the following information to help identify the origin of any hash set within the KFF

- The NSRL hash sets do not begin with “ZZN” or “ZN”. In addition, in the AD Lab KFF, all the NSRL hash set names are appended (post-fixed) with multi-digit numeric identifier. For example: “Password Manager & Form Filler 9722.”
- All HashKeeper Alert sets begin with “ZZ”, and all HashKeeper Ignore sets begin with “Z”. (There are a few exceptions. See below.) These prefixes are often followed by numeric characters (“ZZN” or “ZN” where N is any single digit, or group of digits, 0-9), and then the rest of the hash set name. Two examples of HashKeeper Alert sets are:
  - “ZZ00001 Suspected child porn”
  - “ZZ14W”

  An example of a HashKeeper Ignore set is:
  - “Z00048 Corel Draw 6”
- The DHS collection is broken down as follows:
  - In 1.81.4 and later there are two sets named “DHS-ICE Child Exploitation JAN-1-08 CSV” and “DHS-ICE Child Exploitation JAN-1-08 HASH”.
  - In AD Lab there is just one such set, and it is named “DHS-ICE Child Exploitation JAN-1-08”.

Once an investigator has identified the vendor from which a hash set has come, he/she may need to consider the vendor’s philosophy on collecting and categorizing hash sets, and the methods used by the vendor to gather hash values into sets, in order to determine the relevance of Alert (and Ignore) hits to his/her project. The following descriptions may be useful in assessing hits.

NIST NSRL

The NIST NSRL collection is described at: http://www.nsrl.nist.gov/index.html. This collection is much larger than HashKeeper in terms of the number of sets and the total number of hashes. It is composed entirely of hash sets being generated from application software. So, all of its hash sets are given Ignore status by AccessData staff except for those whose names make them sound as though they could be used for illicit purposes.

The NSRL collection divides itself into many sub-collections of hash sets with similar names. In addition, many of these hash sets are “empty”, that is, they are not accompanied by any hash values. The size of the NSRL collection, combined with the similarity in set naming and the problem of empty sets, allows AccessData to modify (or selectively alter) NSRL’s own set names to remove ambiguity and redundancy.

Find contact info at http://www.nsrl.nist.gov/Contacts.htm.

NDIC HashKeeper

NDIC’s HashKeeper collection uses the Alert/Ignore designation. The Alert sets are hash values contributed by law enforcement agents working in various jurisdictions within the US - and a few that apparently come from Luxemburg. All of the Alert sets were contributed because they were believed by the contributor to be connected to child pornography. The Ignore sets within HashKeeper are computed from files belonging to application software.

During the creation of KFF, AccessData staff retains the Alert and Ignore designations given by the NDIC, with the following exceptions. AccessData labels the following sets Alert even though HashKeeper had assigned them as Ignore: “Z00045 PGP files”, “Z00046 Steganos”, “Z00065 Cyber Lock”, “Z00136 PGP Shareware”, “Z00186 Misc Steganography Programs”, “Z00188 Wiping Programs”. The names of these sets may suggest the intent to conceal data on the part of the suspect, and AccessData marks them Alert with the assumption that investigators would want to be “alerted” to the presence of data obfuscation or elimination software that had been installed by the suspect.

The following table lists actual HashKeeper Alert Set origins:

A Sample of HashKeeper KFF Contributions

Hash	Contributor	Location	Contact Information	Case/Source
ZZ00001 Suspected child porn	Det. Mike McNown & Randy Stone	Wichita PD		
ZZ00002 Identified Child Porn	Det. Banks	Union County (NJ) Prosecutor's Office	(908) 527-4508	case 2000S-0102
ZZ00003 Suspected child porn	Illinois State Police			
ZZ00004 Identified Child Porn	SA Brad Kropp, AFOSI, Det 307		(609) 754-3354	Case # 00307D7-S934831

A Sample of HashKeeper KFF Contributions (Continued)

Hash	Contributor	Location	Contact Information	Case/Source
ZZ00000, suspected child porn	NDIC			
ZZ00005 Suspected Child Porn	Rene Moes, Luxembourg Police		rene.moes@police.etat.lu	
ZZ00006 Suspected Child Porn	Illinois State Police			
ZZ00007b Suspected KP (US Federal)				
ZZ00007a Suspected KP Movies				
ZZ00007c Suspected KP (Alabama 13A-12-192)				
ZZ00008 Suspected Child Pornography or Erotica	Sergeant Purcell	Seminole County Sheriff's Office (Orlando, FL, USA)	(407) 665-6948, dpurcell@seminolesheriff.org	suspected child pornogrpahy from 20010000850
ZZ00009 Known Child Pornography	Sergeant Purcell	Seminole County Sheriff's Office (Orlando, FL, USA)	(407) 665-6948, dpurcell@seminolesheriff.org	200100004750
ZZ10 Known Child Porn	Detective Richard Voce CFCE	Tacoma Police Department	(253)594-7906, rvoce@ci.tacoma.wa.us	
ZZ00011 Identified CP images	Detective Michael Forsyth	Baltimore County Police Department	(410)887-1866, mick410@hotmail.com	
ZZ00012 Suspected CP images	Sergeant Purcell	Seminole County Sheriff's Office (Orlando, FL, USA)	(407) 665-6948, dpurcell@seminolesheriff.org	
ZZ0013 Identified CP images	Det. J. Hohl	Yuma Police Department	928-373-4694	YPD02-70707

A Sample of HashKeeper KFF Contributions (Continued)

Hash	Contributor	Location	Contact Information	Case/Source
ZZ14W	Sgt Stephen May		Tamara.Chandler@oag.state.tx.us, (512)936-2898	TXOAG 41929134
ZZ14U	Sgt Chris Walling		Tamara.Chandler@oag.state.tx.us, (512)936-2898	TXOAG 41919887
ZZ14X	Sgt Jeff Eckert		Tamara.Chandler@oag.state.tx.us, (512)936-2898	TXOAG Internal
ZZ14I	Sgt Stephen May		Tamara.Chandler@oag.state.tx.us, (512)936-2898	TXOAG 041908476
ZZ14B	Robert Britt, SA, FBI		Tamara.Chandler@oag.state.tx.us, (512)936-2898	TXOAG 031870678
ZZ14S	Sgt Stephen May		Tamara.Chandler@oag.state.tx.us, (512)936-2898	TXOAG 041962689
ZZ14Q	Sgt Cody Smirl		Tamara.Chandler@oag.state.tx.us, (512)936-2898	TXOAG 041952839
ZZ14V	Sgt Karen McKay		Tamara.Chandler@oag.state.tx.us, (512)936-2898	TXOAG 41924143
ZZ00015 Known CP Images	Det. J. Hohl	Yuma Police Department	928-373-4694	YPD04-38144
ZZ00016	Marion County Sheriff's Department		(317) 231-8506	MP04-0216808

The basic rule is to always consider the source when using KFF in your investigations. You should consider the origin of the hash set to which the hit belongs. In addition, you should consider the underlying nature of hash values in order to evaluate a hit's authenticity.

Higher Level KFF Structure and Usage

Since hash set groups have the properties just described (and because custom hash sets and groups can be defined by the investigator) the KFF mechanism can be leveraged in creative ways. For example:

- You could define a group of hash sets created from encryption software and another group of hash sets created from child pornography files. Then, you would apply only those groups while processing.
- You could also use the Ignore status. You are about to process a hard drive image, but your search warrant does not allow inspection of certain files within the image that have been previously identified. You could do the following and still observe the warrant:
  - 4a. Open the image in Imager, navigate to each of the prohibited files, and cause an MD5 hash value to be computed for each.
  - 4b. Import these hash values into custom hash sets (one or more), add those sets to a custom group, and give the group Ignore status.
  - 4c. Process the image with the MD5 and KFF options, and with AD_Alert, AD_Ignore, and the new, custom group selected.
  - 4d. During post-processing analysis, filter file lists to eliminate rows representing files with Ignore status.

Hash Set Categories

The highest level of the KFF's logical structure is the categorizing of hash sets by owner and scope. The categories are AccessData, Project Specific, and Shared.

Hash Set Categories

Category	Description
AccessData	The sets shipped with as the Library. Custom groups can be created from these sets, but the sets and their status values are read only.
Project Specific	Sets and groups created by the investigator to be applied only within an individual project.
Shared	Sets and groups created by the investigator for use within multiple projects all stored in the same database, and within the same application schema.

Important: Coordination among other investigators is essential when altering Shared groups in a lab deployment. Each investigator must consider how other investigators will be affected when Shared groups are modified.

What has Changed in Version 5.6

WIth the 5.6 release of eDiscovery, and FTK-based products, the KFF feature has been updated.

If you used KFF with applications version 5.5 or earlier, you will want to be aware of the following changes in the KFF functionality.

Changes from version 5.5 to 5.6

Item	Description
KFF Server	KFF Server now runs a different service. • In 5.5 and earlier, the KFF Server ran as the *KFF Server* service. • In 5.6 and later, the KFF Server uses the *AccessData Elasticsearch Windows Service*. For applications version 5.6 and later, all KFF data must be created in or imported into the new KFF Server.
KFF Migration Tool	This is a new tool that lets you migrate custom KFF data from 5.5 and earlier to the new KFF Server. NIST NSRL, NDIC HashKeeper, or DHS library data from 5.5 will not be migrated. You must re-import it. See Migrating Legacy KFF Data on page 266.
KFF Import Utility	This is a new utility that lets you import large amounts of KFF data quicker than using the import feature in the application. See Using the KFF Import Utility on page 269.
KFF Libraries, Templates, and Groups	In 5.5, all Hash Sets were configured within KFF Libraries. KFF Libraries could then contain KFF Groups and KFF Templates. KFF Libraries and Templates have been eliminated. You now simply create or import KFF Groups and add Hash Sets to the groups. You can now nest KFF Groups.
NIST NSRL, NDIC HashKeeper, or DHS libraries	In 5.5 and earlier, to use these libraries, you ran an installation wizard for each library. You now import these libraries using the KFF Import Utility. See About Importing Pre-defined KFF Data Libraries on page 271.
Import Log	FTK-based products no longer include the Import Log.
Export	When you export KFF data you can now choose two formats: • CSV format which replaced XML format • A new binary format See About CSV and Binary Formats on page 275.

Part 4

Reviewing Cases

This part contains information about reviewing cases and contains the following chapters:

- Using the Examiner Interface (page 287)
- Exploring Evidence (page 289)
- Examining Evidence in the Overview Tab (page 306)
- Examining Email (page 311)
- Examining Graphics (page 315)
- Examining Miscellaneous Evidence (page 332)
- Bookmarking Evidence (page 364)
- Searching Evidence with Live Search (page 376)
- Searching Evidence with Index Search (page 387)
- Using Visualization (page 418)
- Examining Volatile Data (page 411)
- Customizing the Examiner Interface (page 476)
- Working with Evidence Reports (page 486)

Chapter 18

Using the Examiner Interface

About the Examiner

You can use the examiner to locate, organize, and export data. The *Examiner* interface contains tabs, each with a specific focus. Most tabs also contain a common toolbar and file list with customizable columns. Additional tabs can be user-defined.

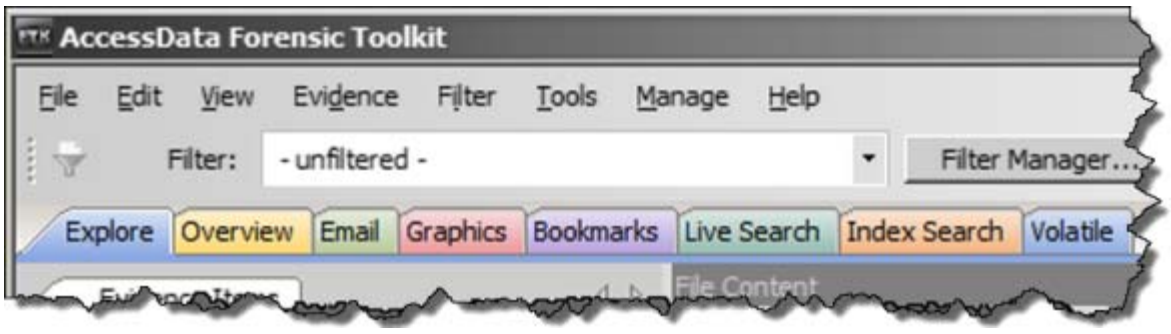
For example, you can use the following tabs to perform a specific task:

- The *Overview* tab lets you narrow your search to look through specific document types, or to look for items by status or file extension.
- The *Graphics* tab lets you quickly scan through thumbnails of the graphics in the case.
- The *Email* tab lets you view emails and attachments.

As you find items of interest, you can do the following

- Create, assign, and view labels in a sorted file list view.
- Use searches and filters to find relevant evidence.
- Create bookmarks to easily group the items by topic or keyword, find those items again, and make the bookmarked items easy to add to reports.
- Export files as necessary for password cracking or decryption, then add the decrypted files back as evidence.
- Add external, supplemental files to bookmarks that are not otherwise part of the case.

Tabs of the Examiner



Note: When entering the Examiner and clicking on a tab for the first time, if that tab uses the Thumbnail pane memory is allocated for displaying graphics and video thumbnails if they are present in the case.

Tabs of the Examiner

Option	Description
Explore Tab	See Explorer Tree Pane (page 289)
Overview Tab	See Using the Overview Tab (page 306)
Email Tab	See Using the Email Tab (page 311)
Graphics Tab	See Using the Graphics Tab (page 315)
Video Tab	See Examining Videos (page 326)
Internet/Chat	See Examining Internet Artifact Data (page 345)
Bookmarks Tab	See Using the Bookmarks Tab (page 371)
Live Search Tab	See Conducting a Live Search (page 376)
Index Tab	See Conducting an Index Search (page 388)
System Information	See Viewing System Information (page 403)
Volatile Tab	See Using the Volatile Tab (page 412)

Also, see Menus of the Examiner (page 61)

Miscellaneous types of evidence

See Examining Miscellaneous Evidence on page 332.

Creating Screen Captures in the Examiner

You can capture screen shots within the Examiner interface. You can include the screen captures when creating reports. You can use screen captures to include information that is not easy to export or include in reports.

See Adding Screen Captures from Examiner on page 496.

Chapter 19

Exploring Evidence

The Explore tab displays all the contents of the case evidence files and drives as the original user would have seen them.

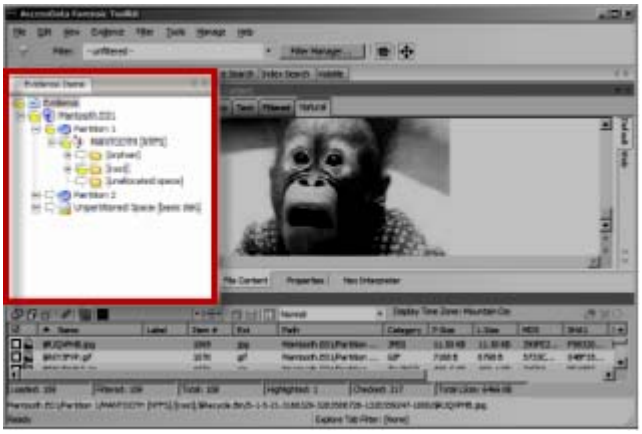
This chapter includes the following topics

- Explorer Tree Pane (page 289)
- File List Pane (page 290)
- The File Content Viewer Pane (page 296)
- The Filter Toolbar (page 304)
- Using QuickPicks (page 305)

Explorer Tree Pane

Lists directory structure of each evidence item, similar to the way one would view directory structure in Windows Explorer. An evidence item is a physical drive, a logical drive or partition, or drive space not included in any partitioned drive, as well as any file, folder, or image of a drive, or mounted image.

The Explorer Tree Pane



File List Pane

Displays case files and pertinent information about files, such as filename, file path, file type and many more properties as defined in the current filter. The files here may display in a variety of colors.

They are as follows:

Black = Default

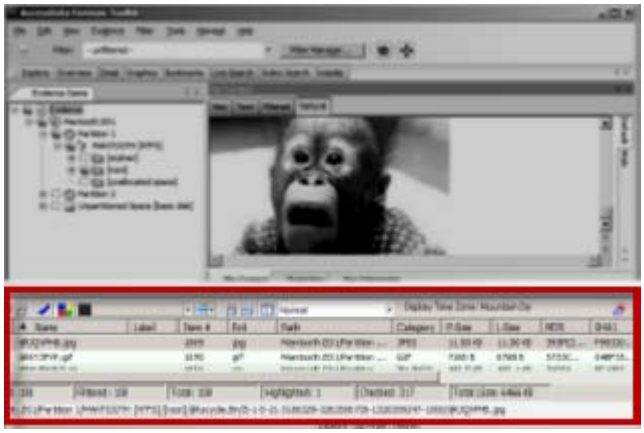
Grey = Deleted

Pink = Bookmarked

Red = Encrypted

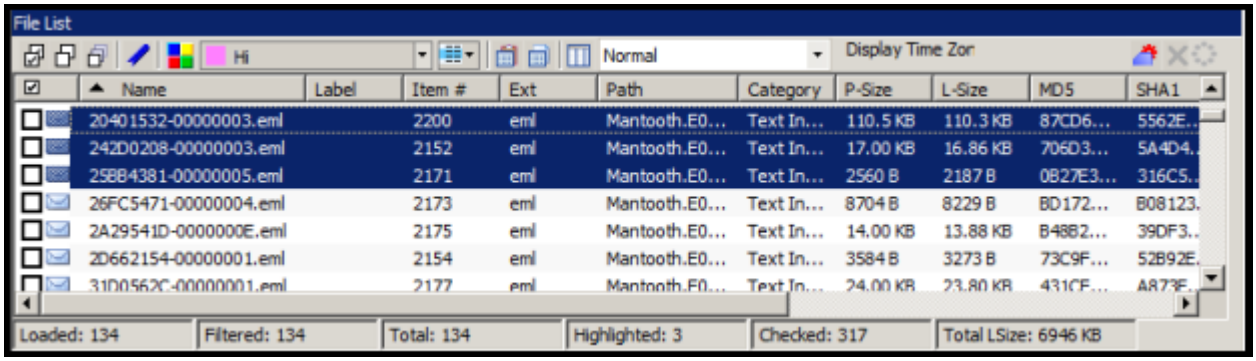
The File List view reflects the files available for the current tabbed view and the properties that meet selected Column templates, limited by any filters that may be applied. In this pane, you can choose which columns to display, as well as the order of those columns, create Bookmarks, create Labels, Copy or Export File Lists. The File List pane is included in all default tab views.

The File List Pane



Using the File List's Columns

For each evidence item, you can diplay multiple columns of informaion about that item.



You can hover over a column's short name to display a tooltip that shows a more descriptive column long name.

You can sort the list using any column. Click on a column heading in the File List view to sort on that column. Hold down the Shift key while clicking a different column header to make the newly selected column the primary-sorted column, while the previous primary-sorted column becomes the secondary-sorted column. There are only two levels of column sorting, primary and secondary.

To undo a secondary sort, click on a different column header to make it the primary-sorted column.

Column widths in most view panes can be adjusted by hovering the cursor over the column heading borders, and dragging the column borders wider or narrower.

See Customizing File List Columns (page 481).

A data box displays in the lower-right of the File List View that indicates the total logical size of the currently listed files.

Using the File List's Type-Down Control Feature

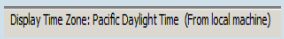
When you view data in the File List, use can use a type-down control feature to locate information. To use the type-down control feature, select any file in the file list and then type the first letters of a file. As you continue to type, the file selector moves to the file list to the closest match to what you type.

Icons of the File List Tool Bar

File List Tool Bar

Component	Description
	Checks all of the files in the current list.
	Unchecks all of the files in the current list.
	Unchecks all of the files in the current case.
	Opens the *Create New Bookmark* dialog.
	Opens the *Manage Labels* dialog.
	Apply Label drop-down allows you to select from the list of defined labels and apply it to a single selected file or a group of files as selected in the **Apply Label To** drop-down.
	Select Label Target drop-down allows you to specify currently Highlighted, Checked, or Listed files for the Label you choose from the Apply Label drop-down.
	Export File List lets you save selected files to another folder.
	Opens the *Copy Special* dialog.
	Opens the *Column Settings* dialog.

File List Tool Bar (Continued)

Component	Description
	Column Templates Sets the columns to a specific selection from the list of defined column sets. See Managing Columns on page 481. Some Default Column Templates are: • Cerberus Results See Cerberus Columns on page 232. • eDiscovery • eDiscovery Mail • Email • Explicit Image Detection (EID) • File Listing • GeoEXIF, GeoIP, Geolocation - Shows Geolocation-related columns See Using Geolocation Columns in the Item List on page 460. • Internet History See Examining Internet Artifact Data on page 345. • Normal (default) • Reports: File Path Section • Reports: Standard
	Displays the selected Time Zone from the local machine.
	Opens the Heatmap page. See Using Visualization Heatmap on page 445.
	Opens the Geolocation page. See Using Visualization Geolocation on page 453.
	Opens the Visualization page. See Using Visualization on page 418.
	Leave query running when switching tabs (this may affect the performance of other tabs).
	Cancel retrieving row data. This is not a pause button. To retrieve row data after clicking **Cancel**, you must begin again. There is no way to pause and restart the retrieval of row data.
	Active spinner indicates Processing activity.

Note: When checking files in a case, these two rules apply:

- Checked files are persistent and remain checked until the user unchecks them.
- Checked files are per-user; another user or an Administrator will not see your checked files as checked when viewing the same case.

File List View Right-Click Menu

When you right-click on any item in the File List view, a menu with the following options appears. Some options are enabled or disabled, depending on the tab you are in, the evidence that exists in the case, the item you have selected, or whether bookmarks have been created.

File List View Right-Click Menu Options

Option	Description
Open	Opens the selected file.
Launch in Content Viewer	Launches the file in the Content Viewer, formerly known as Detached Viewer.
Open With	Opens the file. Choose either Internet Explorer or an External Program.
Create Bookmark	Opens the *Create New Bookmark* dialog for creating a new bookmark.
Add to Bookmark	Opens the *Add to Bookmark* dialog for adding selected files to an existing bookmark.
Remove from Bookmark	Removes a file from a bookmark. From the Bookmarks tab, open the bookmark containing the file to be removed, then select the file. Right-click and select **Remove from Bookmark**.
Labels	Opens the *Labels* dialog. View assigned Labels, create or delete a Label, Apply a Labels to file, or Manage Local or Manage Global Labels.
Review Labels	Opens the *Label Information* dialog to display all labels assigned to the selected file or files.
Mount Image to Drive	Allows you to mount an image logically to see it in Windows Explorer, or physically to view.
Add Decrypted File	Right-click and select **Add Decrypted File**. Opens the *Add Decrypted File* dialog. Browse to and select the file to add to the case, click **Add**.
View File Sectors	Opens a hex view of the selected file. Type in the file sector to view and click **Go To**.
Find on Disk	Opens the Disk Viewer and shows where the file is found in the disk/file structure. **Note:** Find on disk feature won't find anything under 512 B physical size. Files smaller than 1500 bytes may reside in the MFT and do not have a start cluster. Find on disk depends on that to work.
Find Similar Files	Opens the *Search for Similar Files* dialog. The selected file's hash value is displayed. Click **From File** to see the filename the hash is from. The Evidence Items to Search box shows all evidence items in the case. Mark which ones to include in the search. Select the Minimum Match Similarity you prefer, and click **Search** or **Cancel**.
Open in Registry Viewer	Opens a registry file in AccessData's Registry Viewer. Choose SAM, SOFTWARE, SYSTEM, SECURITY, or NTUSER.dat.
Export	Opens the *Export* dialog with all options for file export, and a destination path selection.
Export to Image	Opens the *Create Custom Content* Image dialog.

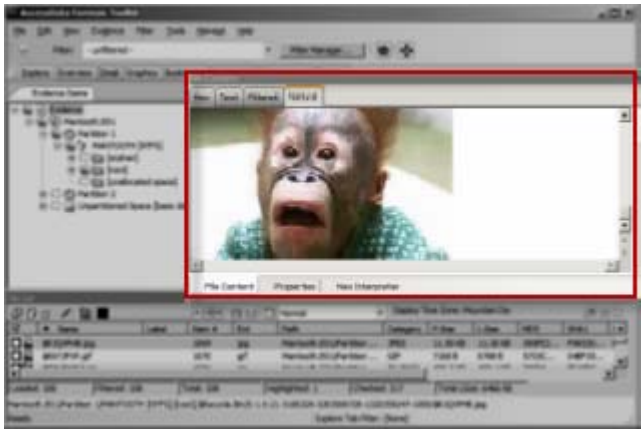
File List View Right-Click Menu Options (Continued)

Option	Description
Acquire to Disk Image	Allows you to create a new disk image (001, AFF, E01, or S01) from a disk image in the case.
Export File List Info	Opens the *Save As* dialog. Choose TXT, TSV, or CSV. The default name is FileList.TXT.
Copy Special	Opens the *Copy Special* dialog.
Check All Files in Current List	Check-marks all files in the current list.
Uncheck all Files in Current List	Unchecks all files in the current list.
Uncheck All Files in Case	Unchecks all files in the case.
Check/Uncheck All Highlighted	Checks or unchecks all files that are currently highlighted in the list. (Pressing the space bar does the same thing.)
Change “Flag as Ignorable” Status	Change Flag Status of all files as either Ignorable or Not Ignorable according to Selection Options.
Change “Flag as Privileged” Status	Change Flag Status of all files as either Privileged or Not Privileged according to Selection Options.
Re-assign File Category	Change File Category assignment.
View This Item In a Different List	Changes the File List view from the current tab to that of the selected tab from the pop-out.

The File Content Viewer Pane

Displays the contents of the currently selected file from the File List. The Viewer toolbar allows the choice of different view formats.

The File Content Viewer Pane



You can use CTRL+F to search within the File Content pane.

The File Content pane tab has a *Default* tab and a *Web* tab for each of the following tabbed views:

- Hex Tab
- Text Tab
- Filtered Tab
- Natural Tab
- Properties Tab
- Hex Interpreter Tab

Tabs of the File Content Pane

Note: The Find on Disk feature (in File List view, right-click an item) won't find anything under 512 Bytes physical size. Also, files smaller than 1500 bytes may reside in the MFT and thus do not have a start cluster. Find on Disk depends on the start cluster information to work.

Note: In the File List view of any tab, a much-greater-than symbol (>>) denotes that the path is not an actual path, but that the file came from another file or source, such as a zipped, compressed, or linked (OLE) file, or that it was carved.

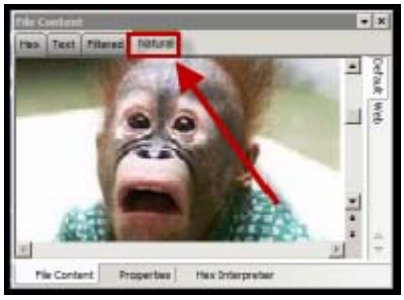
The File Content pane title changes depending on which tab is selected at the bottom of the window. The available tabs are File Content, Properties, and Hex Interpreter. These three tabs default to the bottom left of the File Content pane in any program tab where it is used.

The three tabs can be re-ordered by clicking on a tab and dragging-and-dropping it to the position in the linear list where you want it. Click any of these tabs to switch between them. The information displayed applies to the currently selected file in the Viewer pane.

The Natural Tab

The Natural tab displays a file's contents as it would appear normally. This viewer uses INSO filters for viewing hundreds of file formats without the native application being installed.

FIle Content Pane: Natural Tab

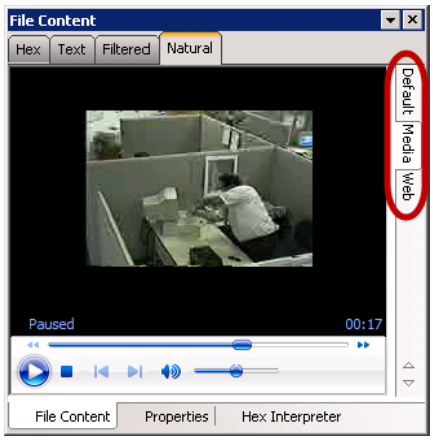


Note: When highlighting terms in Natural View, each term throughout the document is highlighted, one term at a time. When it reaches the limit of highlighting in that window, regardless of which term it is on (first, second, third, etc.) it stops highlighting. There is no workaround.

Note: Viewing large items in their native applications may be faster than waiting for them to be rendered in the *Examiner* viewer.

The Natural View top tab is the only one of the four that has additional tabs that provide for the viewing of Text, Media, and Web files, in their native application environment.

File Content Pane: Default, Media, and Web Tabs



- Natural Tab: Default

  The Default tab displays documents or files in a viewer that uses INSO (Inside-Out) Technology, according to their file type.

- Natural Tab: Media

  Case audio and video files play using an embedded Windows Media Player.

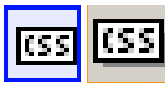
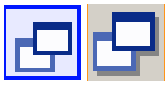
  The *Examiner* has the functionality to recognize popular mobile phone formats (found in many MPE images) such as M4A, MP4, AMR, and 3GP. These file types play inside the Media tab as long as the proper codecs are installed that would also allow those files to play in Windows Media Player.

- Natural Tab: Web

  The Web view uses an embedded Internet Explorer instance to display the contents of the selected file in a contained field.

  In the Web view, the top-left border of the pane holds two toggle buttons for enabling or disabling HTML content.

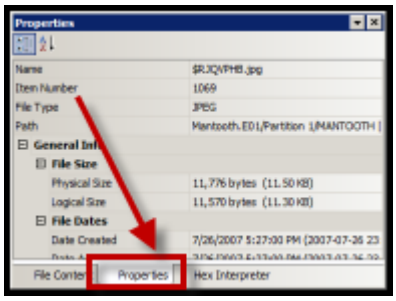
Natural Tab: Web Tab Toggle Buttons

	Enable or Disable CSS Formatting. CSS formatting displays any fonts, colors, and layout from cascading style sheets. HTML formatting not part of a cascading style sheet might remain. Enabled feature is indicated by a blue background; disabled feature is indicated by a gray background.
	Enable or Disable External Hyperlinks. Enabled hyperlinks in the file will link to active internet pages. This may not accurately provide data that was available using that link at the time the image was made, or the evidence was acquired. Enabled feature is indicated by a blue background; disabled feature is indicated by a gray background.

The Properties Tab

The Properties tab is found in the File Content View, and displays a pane, or window of information about a selected file. The following figure displays the information contained in the Properties pane. This information corresponds to the file selected in the *File List* pane.

The Properties Tab



Properties Pane Components

Option	Description
Name	The filename of the selected file.
Item Number	A number assigned to the item during evidence processing.
File Type	The type of a file, such as an HTML file or a Microsoft Word 98 document. The file header is used to identify each item's file type.
Path	The path from the evidence source down to the selected file.
General Info	General information about the selected file: *File Size*: Lists the size attributes of the selected file as follows: • Physical size of the file, including file slack • Logical size of the file, excluding file slack *File Dates*: Lists the Dates and Times of the following activities for that file on the imaged source: • Created • Last accessed • Last modified All dates with times are listed in UTC and local times.
File Attributes	The attributes of the file:
	General: • *Actual File*: True if an actual file. False if derived from an actual file. • *From Recycle Bin:* True if the file was found in the Recycle Bin. False otherwise. • *Start Cluster:* Start cluster of the file on the disk. • *Compressed*: True if compressed. False otherwise. • *Original Name*: Path and filename of the original file. • *Start Sector*: Start sector of the file on the disk. • *File has been examined for slack*: True if the file has been examined for slack. False otherwise.
	DOS Attributes: • *Hidden*: True if Hidden attribute was set on the file. False otherwise. • *System*: True if this is a DOS system file. False otherwise. • *Read Only*: True or False value. • *Archive*: True if Read Only attribute was set on the file. False otherwise. • *8.3 Name*: Name of the file in the DOS 8.3 naming convention, such as [filename.ext].

Properties Pane Components (Continued)

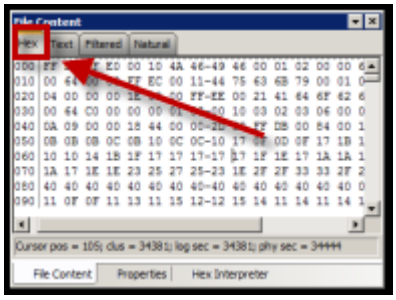
Option	Description
	Verification Hashes: True if verification hashes exist. False otherwise.
	NTFS Information: • *NTFS Record Number*: The number of the file in the NTFS MFT record. • *Record Date*: UTC time and date record was last modified. • *Resident*: True if the item was Resident, meaning it was stored in the MFT and the entire file fit in the available space. False otherwise. (If false, the file would be stored FAT fashion, and its record would be in the $I30 file in the folder where it was saved.) • *Offline*: True or False value. • *Sparse*: True or False value. • *Temporary*: True if the item was a temporary file. False otherwise. • *Owner SID*: The Windows-assigned security identifier of the owner of the object. • *Owner Name*: Name of the owner of that file on the source system. • *Group SID*: The Windows-assigned security identifier of the group that the owner of the object belongs to. • *Group Name*: The name of the group the owner of the file belongs to.
	NTFS ACL attributes. This is the same functionality that is currently found in Imager. When there are multiple sets of ACL attributes present, they are now distinguished by number.
File Content Info	The content information and verification information of the file: • *MD5 Hash*: The MD5 (16 bytes) hash of the file (default). • *SHA-1 Hash*: The SHA-1 (20 bytes) hash of the file (default). • *SHA-256 Hash*: the SHA-256 (32 bytes) hash of the file (default).

The information displayed in the Properties tab is file-type-dependent, so the selected file determines what displays.

The Hex Tab

The Hex tab shows the file content in hexadecimal. It is different from the Hex Interpreter tab at the bottom of the screen.

The Hex Tab



The bar symbol indicates that the character font is not available, or that an unassigned space is not filled.

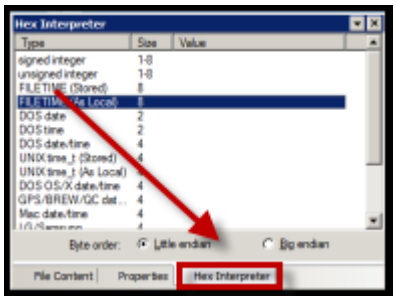
File Content Hex View Right-click Menu Options

Select all	*Show decimal offsets*
Copy text	*Show text only*
Copy hex	*Fit to window*
Copy Unicode	*Save current settings*
Copy raw data	*Go to Offset* takes you to a desired offset. You can select the Hex data to save as a separate file.
Save selection	*Save selection as carved file* lets you manually carve data from files.

The Hex Interpreter Tab

The Hex Interpreter tab shows interpreted hexadecimal values selected in the Hex tab viewer on the File Content tab in the Viewer pane into decimal integers and possible time and date values as well as Unicode strings.

The Hex Interpreter Tab



The Hex Value Interpreter reads date/time stamp values, including AOL date/time, GPS date/time, Mac date/time, BCD, BCD Hex, and BitDate.

The Hex tab displays file contents in hexadecimal format. Use this view together with the Hex Interpreter pane. The Hex View tab is also found in the File Content View. This feature helps if you are familiar with the internal code structure of different file types, and know where to look for specific data patterns or for time and date information.

To convert hexadecimal values

1. Highlight one to eight continuous bytes of hexadecimal code in the **File Content pane > File Content tab viewer > Hex tab**. (Select two or more bytes for the Unicode string, depending on the type of data you want to interpret and view.)
2. Switch to the Hex Interpreter tab at the bottom of the **File Content Viewer > Hex tab**, or open it next to, or below the **File Content tab > Hex tab** view to see both concurrently.
3. The possible valid representations, or interpretations, of the selected code automatically display in the Hex Value Interpreter.

Little-endian and big-endian refers to which bits are most significant in multi-byte data types, and describes the order in which a sequence of bytes is stored in a computer's memory. Microsoft Windows generally runs as Little Endian, because it was developed on and mostly runs on Intel-based, or Intel-compatible machines.

In a big-endian system, the most significant bit value in the sequence is stored first (at the lowest storage address). In a little-endian system, the least significant value in the sequence is stored first. These rules apply when reading from left to right, as we do in the English language.

As a rule, Intel based computers store data in a little-endian fashion, where RISC-based systems such as Macintosh, store data in a big-endian fashion. This would be fine, except that a) AccessData's products image and process data from both types of machines, and b) there are many applications that were developed on one type of system, and are now "ported" to the other system type. You can't necessarily apply one rule and automatically know which it is.

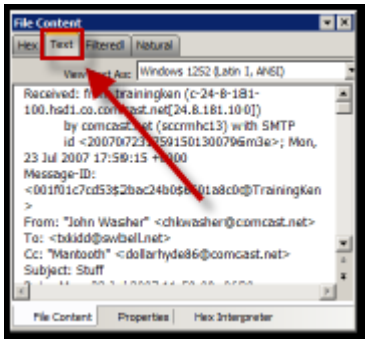
Little-endian is used as the default setting. If you view a data selection in the Hex Interpreter and it does not seem correct, you can try choosing the big-endian setting to see if the data displayed makes more sense.

The Text Tab

The Text tab displays the file's content as text using the code page selected from the *View Text As* drop-down menu.

The File Content pane currently provides many code pages from which to choose. When the desired code page is selected, the Text tab will present the view of the selected file in text using the selected code page language.

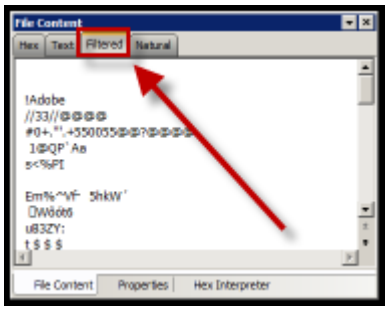
The Text Tab



The Filtered Tab

The Filtered tab shows the file's text created during indexing. The following figure represents content displayed in the filtered tab. The text is taken from an index created for the current session if indexing was not previously selected.

The Filtered Tab


File Content
Hex
Text
Filtered
Natural
!Adobe
u83ZY:
File Content
Properties
Hex Interpreter

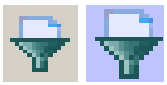
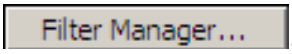
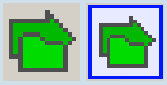
The Filter Toolbar

The interface provides a tool bar for applying QuickPicks and Filters to the case.

See also Filtering Data to Locate Evidence (page 158)

The Filter Toolbar

Filter Toolbar Components

Component	Description
	Turns the filter on or off. Filtered data is shown in a colored pane to indicate that it is filtered. In addition, if no filter is applied, the icon is grayed out. When active, or ON, the Filter button has a light blue background. When inactive, or OFF, the background is gray.
	Opens the drop-down menu listing defined filters. Applies the selected filter.
	Opens the Filter Manager. The Filter Manager allow multiple filters to be selected and applied concurrently. These are known as Compound filters.
	Turns the QuickPicks filter on or off. The QuickPicks filter is used in the Explore tab to populate the file list with only items the investigator wishes to analyze. When active, or ON, the QuickPicks button is light blue. When inactive, or OFF, the background is gray.
	Locks or unlocks the movable panes in the application. When the lock is applied, the box turns grey, and the panes are locked. When unlocked, the box has a light blue background and blue outline, indicating the panes can be moved.

Using QuickPicks

QuickPicks is a type of filter that allows the selection of multiple folders and files in order to focus analysis on specific content. The following figure represents the Explore Evidence Items tree with a partially selected set of folders and sub-folders using the QuickPicks feature.

The QuickPicks filter simultaneously displays open and unopened descendent containers of all selected tree branches in the File List at once. The colors of the compound icons indicate whether descendants are selected.

The icons are a combination of an arrow, representing the current tree level, and a folder, representing any descendants.

QuickPicks Icons

	A dark green arrow behind a bright green folder means all descendants are selected.
	A dark green arrow behind a yellow folder means that although the folder itself is not selected, some of its descendents are selected.
	A white arrow with no folder means neither that folder, nor any of its descendants is selected.
	A white arrow behind a bright green folder means that all descendants are selected, but the folder is not.

The File List view reflects the current QuickPicks selections. When QuickPicks is active, or on, if no folders are selected, the File List view shows the currently selected item in the Tree view, including first-level child objects. When any item is selected, that selection is reflected in the File List view. When QuickPicks is not active, or off, the File List view displays only items at the selected level in the tree view, with no children.

Chapter 20

Examining Evidence in the Overview Tab

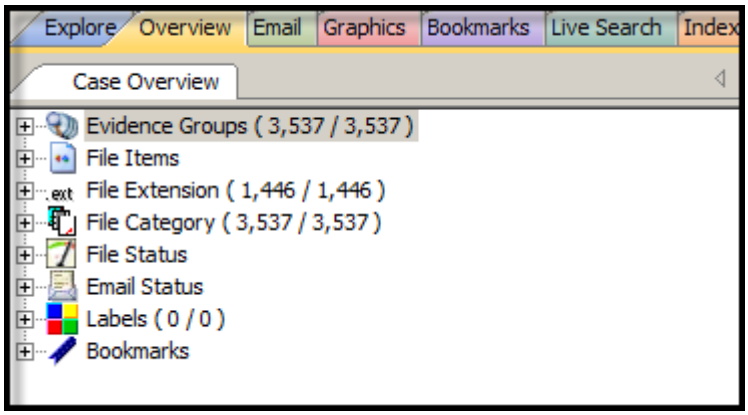
This chapter includes the following topics

- Using the Overview Tab (page 306)

Using the Overview Tab

The Overview tab provides a general view of a case. You can find the number of items in various categories, view lists of items and lists of individual files by category, status, and extension. Evidence categories are represented by trees in the upper-left Case Overview pane of the application.

The Overview Tab



Evidence Groups Container

Evidence items can be assigned to a group when they are added to a case. The Evidence Groups Container shows at-a-glance which Evidence Groups are in use in a case, and the number of items associated with each.

File Items Container

The File Items container itemizes files by whether they have been checked and lists in an expandable tree view the evidence files added to the case.

File Extension Container

The File Extension container itemizes files by their extensions, such as TXT, MAPIMAIL, and DOC and lists them in a tree view.

The File Extension Container content numbers do not synchronize or match up with the overall number of case items. This is because case items, such as file folders, do not have extensions and, therefore, are not listed in the File Extension Container.

File Category Container

File Category container itemizes files by type, such as a word processing document, graphic, email, executable (program file), or folder, and lists them in a tree view.

The statistics for each category are automatically listed. Expand the category tree view to see the file list associated with it.

BlackBerry IPD files (the files created on your PC when you back up your BlackBerry device) are recognized and categorized. Not every BlackBerry device has the same features as all the others, and everyone uses their device differently so there is no guarantee that every type of data will be available from every set of backup IPD files. You will most likely see HTML and XML files, Messages, and Pictures/Photos. Address Books, Tasks, and Calendars will be extracted if available.

File Categories

Archives	Archive files include email archive files, ZIP, STUFFIT, THUMBS.DB thumbnail graphics, and other archive formats.
Databases	Database files such as those from MS Access, Lotus Notes NSF, and other database programs.
Documents	Includes recognized word processing, HTML, WML, XML, TXT, or other document-type files.
Email	Includes email messages from Outlook, Outlook Express, AOL, Endoscope, Yahoo, Rethink, Udder, Hotmail, Lotus Notes, and MSN.
Executables	Includes Win32 executable files and DLLs, OS/2, Windows VxD, Windows NT, Java Script, and other executable formats.
Folders	Folders or directories that are located in the evidence.
Graphics	Lists files having the standard recognized graphic formats such as TIF, GIF, JPEG, and BMP, as found in the evidence.
Internet/Chat Files	Lists Microsoft Internet Explorer cache and history indexes.
Mobile Phone Data	Lists data acquired from recognized mobile phone devices.
Multimedia	Lists AIF, WAV, ASF, and other audio and video files as found in the evidence.
OS/File System Files	Lists partitions, file systems, registry files, and so forth.
Other Encryption Files	Lists found encrypted files, as well as files needed for decryption such as EFS search strings, Public Keys, Private Keys, and other RSA Keys. For more information on Decrypting Encrypted Files, See Decrypting Files (page 181).

File Categories (Continued)

Other Known Types	A miscellaneous category that includes audio files, help files, dictionaries, clipboard files, link files, and alternate data stream files such as those found in Word DOC files, etc. **Note:** Other Known Types includes NSF Misc. Note (Calendar, $profile data, and other miscellaneous files that in the past were shown as HTML), and NSF Stub Note (a link to the same email or calendar item in another view) sub categories.
Presentations	Lists multimedia file types such as MS PowerPoint or Corel Presentation files.
Slack/Free Space	Lists files, or fragments of files that are no longer seen by the file system, but that have not been completely overwritten.
Spreadsheets	Lists spreadsheets from Lotus, Microsoft Excel, Quattro Pro, and others, as found in the evidence.
Unknown Types	Lists files whose types are not identified.
User Types	Lists user-defined file types such as those defined in a Custom File Identification File.

File Status Container

File Status covers a number of file categories that can alert the investigator to problem files or help narrow down a search.

The statistics for each category are automatically listed. Click the category button to see the file list associated with it. The following table displays the file status categories.

File Status Categories

Bad Extensions	Files with an extension that does not match the file type identified in the file header, for example, a GIF image renamed as [graphic].txt.
Data Carved Files	The results of data carving when the option was chosen for preprocessing.
Decrypted Files	The files decrypted by applying the option in the Tools menu. **Note:** Decrypted status means the file was decrypted from evidence added to the case in its original form. The software has had control of the file and knows it was originally encrypted, that it was contained in the original evidence, and thus, is relevant to the case.
Deleted Files	Complete files or folders recovered from slack or free space that were deleted by the owner of the image, but not yet written over by new data.
Duplicate Items	Any items that have an identical hash. Because the hash is independent of the filename, identical files may actually have different filenames. The first instance of a file found during processing is the primary item. Any subsequently found files, whose hash is identical, is considered a secondary item, regardless of how many duplications of the same file are found.
Email Attachments	Files attached to the email in the evidence.
Email Related Items	All email-related files including email messages, archives, and attachments.

File Status Categories (Continued)

Encrypted Files	Files that are encrypted or have a password. This includes files that have a read-only password; that is, they may be opened and viewed, but not modified by the reader. If the files have been decrypted with EFS, and you have access to the user's login password, you can decrypt these files.
Flagged Ignore	Files that are flagged to be ignored are probably not important to the case.
Flagged Privileged	Files that are flagged as privileged cannot be viewed by the Case Reviewer.
From Recycle Bin	Files retrieved from the Windows Recycle Bin.
KFF Alert Files	Files identified as likely to be contraband or illicit in nature.
KFF Ignorable	Files identified as likely to be forensically benign.
OCR Graphics	Files with graphic text that have been interpreted by the Optical Character Recognition engine.
OLE Sub-items	Items or pieces of information that are embedded in a file, such as text, graphics, or an entire file. This includes file summary information (also known as metadata) included in documents, spreadsheets, and presentations.
User Decrypted	Files you've previously decrypted, and then added to the case. **Note:** A user can add any file using Add Decrypted File, and it will be set as decrypted by user. This status indicates that AccessData did not decrypt this file, and cannot guarantee its validity or that such a file has anything to do with the case.

Cluster Topic Container

Cluster Topic are groups of files created through Document Content Analysis. This feature allows you to group Email Threaded data and Near Duplicate data together for quicker review. After the application completes the analysis, the content appears in the *Cluster Topic* container. The content is organized by the keywords in which the documents were analyzed and grouped. Documents that do not fit into a *Content Topic* category are placed in the *UNCLUSTERED* category.

Using Document Content Analysis (page 424)

Processing and Displaying Evidence Counts

When you open the *Examiner* > *Overview* tab, queries are run to calculate the evidence counts in multiple categories: *Evidence Groups*, *File Extension*, *File Category*, and *Labels*. If you have a large case, you can speed up performance by calculating counts in only one category. You can restrict this in one of two ways:

- Through a registry setting
- In the Examiner interface

To Restrict Count Updates by Adding a Settings Entry in the Registry

1. Navigate to the following path in the registry to add the settings value:
   HKEY_CURRENT_USER/Software/AccessData/Products/Forensic Toolkit/5.3/Settings/Tabs/Tab7
2. Add the following value:
   OverviewUpdateType REG_DWORD *2*

Use the data values in the following table to select which category you would like to specify.

Registry Data Values	
FILE CATEGORY	2
FILE EXTENSION	3
LABELS	6
EVIDENCE GROUPS	7

To Restrict Count Updates in the Examiner Interface

1. Click on an item within one of the evidence categories that contain evidence counts.
2. Press the *Home* key on the keyboard.

   This will reduce the case overview tree to only the selected item and it's children. For example, if you select the *Documents* category, this will reduce the case overview tree to showing only *Documents*. This choice is stored in the settings for the Overview tab.

To Restore Full Count Updates in the Examiner Interface

- Click an item in the reduced tree and press the *End* key on the keyboard to restore the full case overview tree.

Disabling the Calculation and Display of the Total Logical Size

When viewing evidence in the Examiner, the Total Logical Size (Total LSize) is calculated for different categories of evidence. To speed up the interface for large cases, you can disable the calculation and display of this value by adding a registry value.

To Hide the Total Logical Size

1. Navigate to the following path in the registry:
   HKLM\SOFTWARE\AccessData\Products\Forensic Toolkit\version
2. Add the following value:
   hide_total_logical_size DWORD value *1*

To Restore the Total Logical Size

- Use the following value:
  hide_total_logical_size DWORD value *0*

Chapter 21

Examining Email

This chapter includes the following topics

- Using the Email Tab (page 311)

Using the Email Tab

The Email tab displays email mailboxes and their associated messages and attachments. The display is a coded HTML format.

The Email Tab

Email Status Tree

The Email Status tree lists information such as the sender of the email, and whether an email has attachments. They are listed according to the groups they belong to.

Email Archives Tree

The *Email Archives* tree lists Email related files that are considered containers. Item types include DBX, MBX, PST/OST, Saved Mail, Sent Mail, Trash, and so forth. The tree is limited to archive types found within the evidence during processing.

Email Tree

The *Email* tree lists message counts, AOL DBX counts, PST counts, NSF counts, MBOX counts, and other such counts.

Exchange and PST Emails can be exported to MSG format. In addition, MSG files resulting from an export of internet email look the way they should.

The **Email Tab > Email** Items tree view contains two new groups: Email By Date (organized by Year, then by Month, then by Date, for both Submitted and Delivered); and Email Addresses (organized by Senders and Recipients, and subcategorized by Email Domain, Display Name, and Email Addresses).

You can also export Tasks, Contacts, Appointments, Sticky Notes, and Journal Entries to MSG files.

Important: If the Mozilla Firefox directory is added as evidence while in use, history, downloads, etc. are identified as zero-length files.

When an email-related item is selected in the File List, right-click and choose **View this item in a different list > Email** to see the file in Email context.

Note: Email data parsed into the new nodes in the Email tree view will only be populated in new cases. Converted cases will not have this data. To make this data available in older cases, re-process the case in the new version.

Examining Windows 10 Email

It is possible to process and view Email and Contacts for Windows 10 Email.

Note: This software does not parse anything other than Email and Contacts for Windows 10 Email at this time.

Processing Windows 10 Email and Contacts

To Process Windows 10 Email and Contacts:

1. In the *Evidence Processing* window, select **Expand Compound Files**.
2. Click on the **Expansion Options** button. Scroll down and select the **Unistore Database (Windows 10 Mail)** option.
3. Click **Ok** and process the evidence.

Viewing Windows 10 Email and Contacts

In the Windows File System, the ESE database is found in the store.vol file within the Unistore DB. This is where the logical structure for emails, contacts, and other important information is kept.

There are two ways to view Windows 10 Email and Contacts. If you choose to see the full file structure of the store.vol file, you will need to use the Explore Tab. If you only want to view emails, the Email Tab contains all emails in the case, including Windows 10 Email.

To View Windows 10 Contacts in the Explore Tab:

1. Process the evidence as described above.
2. Navigate to the *Explore Tab*.
3. In the *Evidence Items* pane, navigate to the user's **EmailComms > Comms > UnistoreDB > store.vol** file. Drill down until you see the email folders.
4. To view contacts, open the folder for the email program you are looking for. Expand the IPM.root folder, then select the Contacts folder. The Contacts will then populate in the File List pane. Select a Contact from the list to see the information associated with that contact in the File Content pane. Select the Properties tab to view the various properties associated with the selected contact in Cool HTML.

To View Windows 10 Email in the Explore Tab:

1. Process the evidence as described above.
2. Navigate to the *Explore Tab*.
3. In the *Evidence Items* pane, navigate to the user's **EmailComms > Comms > UnistoreDB > store.vol** file. Inside this file will be the various email folders.
4. To view emails, expand the IPM.root folder for the email program you are looking for and select the Inbox folder. The list of emails will then populate in the File List pane. Select an email to view it in the File Content pane. Select the Properties tab to view the various properties associated with the selected email.

Note: If you'd like to see an email in the Email Tab instead of the Explore Tab, right-click on the email and select View This Item In a Different List > Email.

To View Windows 10 Email in the Email Tab:

- ❖ Windows 10 Email is automatically populated in the existing folders in the email tab.

Exporting Windows 10 Email

Individual emails can be exported as MSG files. When exported, all existing attachments will be included.

Note: If the user has not downloaded the attachment, the content will not be available.

To Export a Windows 10 Email:

1. Right-click on the item you'd like to export and select **Export**.
2. In the *Export* window, select the **Export emails as MSG** option and set a Destination path.
3. Click **Ok**.
   Your email(s) will be exported to the selected destination folder.

Chapter 22

Examining Graphics

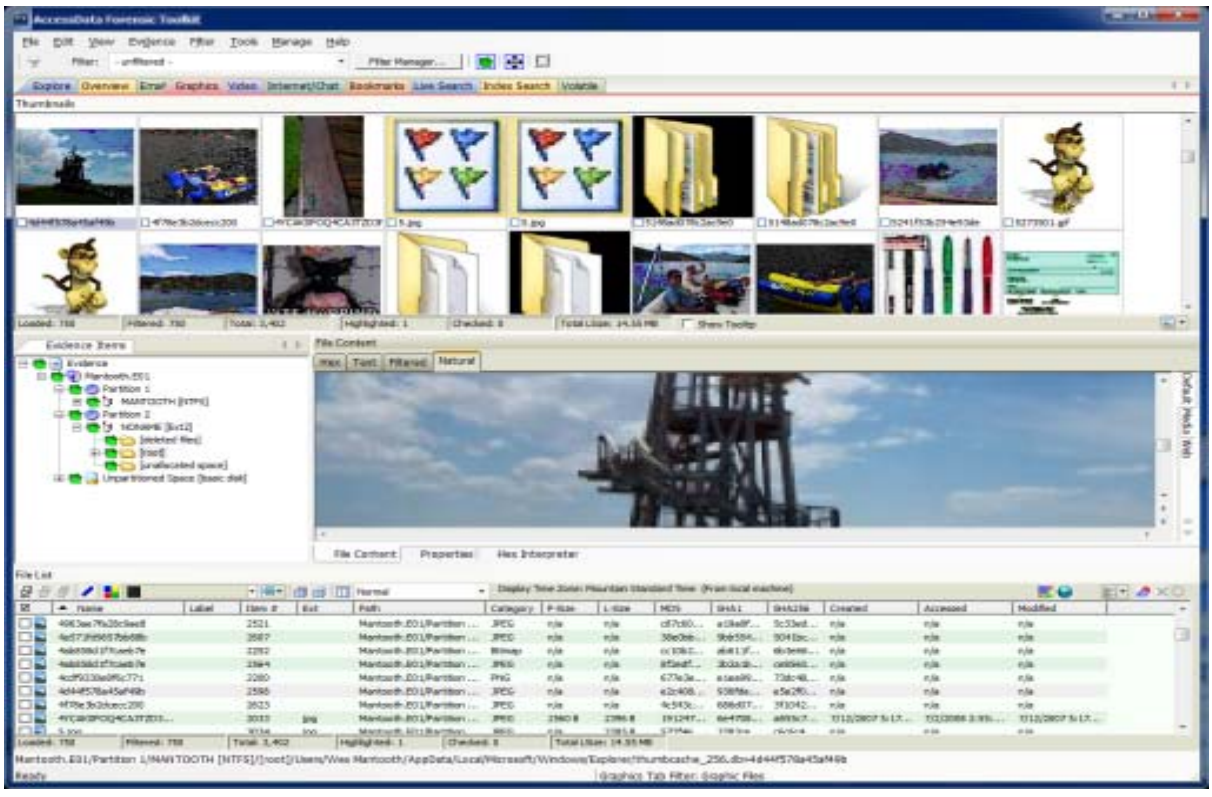
This chapter includes the following topics

- Using the Graphics Tab (page 315)
- Evaluating Explicit Material (page 319)
- Using PhotoDNA to Compare Images (page 322)

Using the Graphics Tab

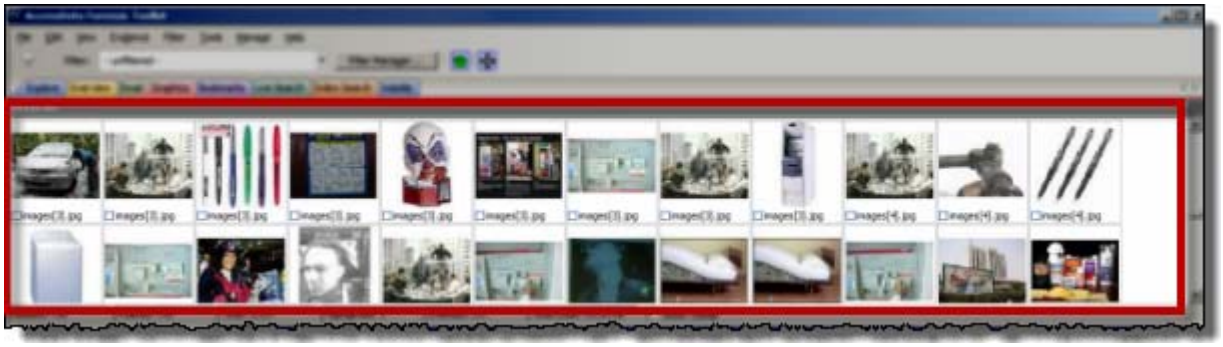
The *Graphics* tab displays the graphics in a case like a photo-album.

The Graphics Tab



Each graphic file is shown in a thumbnail view. A graphic displays in the *Thumbnail* view when its thumbnail is checked in the *File Contents* pane.

Graphics tab Thumbnails



In the thumbnail viewer, if a graphic is not fully loaded, the following icon is displayed:

In the thumbnail viewer, if a graphic cannot be displayed, the following icon is displayed:

Beneath each thumbnail image is a check box. When creating a report, choose to include all of the graphics in the case or only those graphics that are checked.

The Evidence Items pane shows the Overview tree by default. Use the View menu to change what displays here. Only graphic files appear in the File List when the tab filter is applied. Turn off the tab filter to view additional files.

Note: The thumbnail pane needs to be sized at least one thumbnail in height for the scrolling feature to work properly.

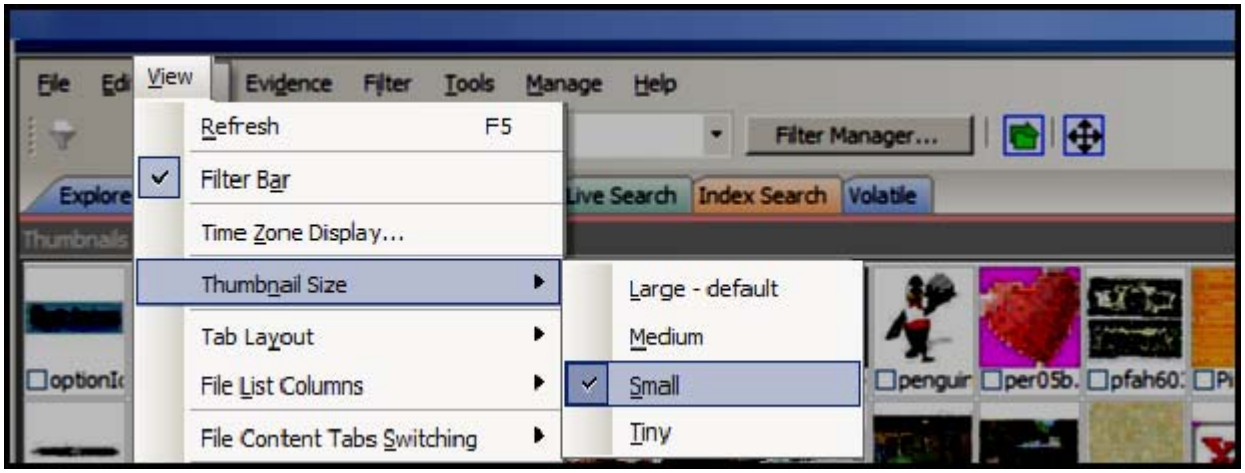
The Thumbnails Size Setting

The thumbnail settings allow large amounts of graphic data to be displayed for evidence investigation, or larger thumbnails to show more detail quickly. The investigator does not always need to see details to pick out evidence; scan the thumbnails for flesh tones, photographic-type graphics, and perhaps particular shapes. Once

found, the graphics can be inspected more closely in the Content Viewer. There are two ways to change the thumbnails size setting, in the *Examiner* View menu or with the Thumbnail Size Selector ( ).

- To change the Thumbnail Size in the View menu, click **View > Thumbnail Size** and select a size.
- To change the Thumbnail Size with the Thumbnail Size Selector, click and select a size.

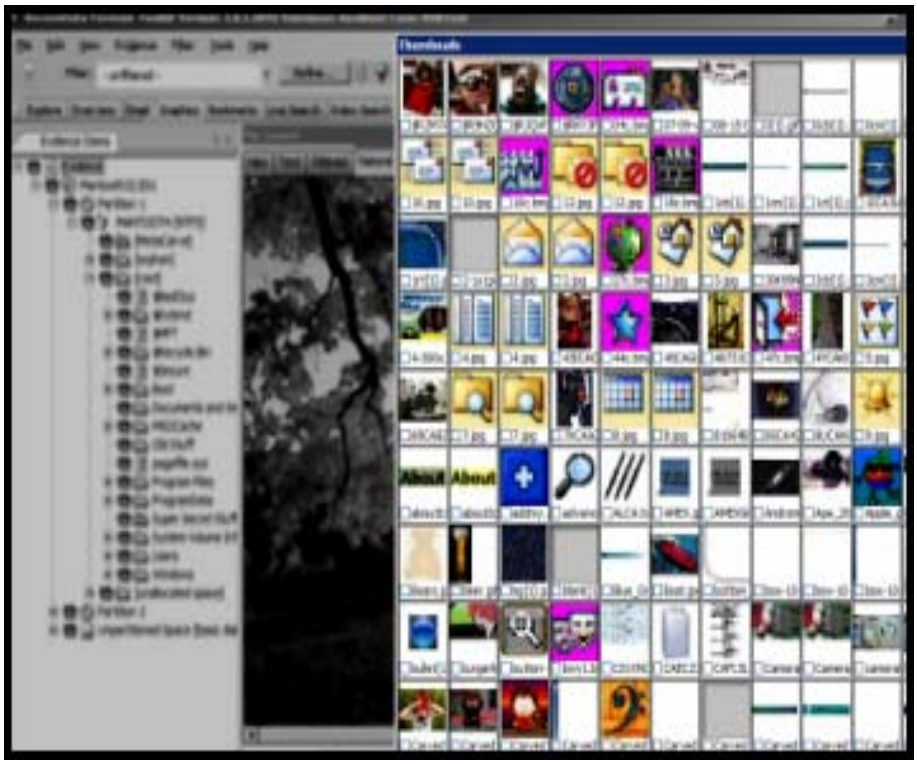
Changing the Thumbnail Size



Moving the Thumbnails Pane

The detachable pane feature is especially useful when you undock the thumbnails graphics pane and move it to a second monitor, thus freeing your first monitor to display the entire data set for the graphics files being analyzed. You can undock the *Thumbnails* pane, and expand it across the screen. Then you can open the Thumbnails Settings sub-menu, and scale the thumbnails down to fit as many as possible in the pane.

Moving the Thumbnails Pane



Evaluating Explicit Material

When explicit material is suspected in a case, the Explicit Image Detection (AID) feature allows for easier location and identification of those files. When creating the case, there are options for identifying explicit material.

See Using Explicit Image Detection (page 96) for more information on setting the EID pre-processing options prior to case creation.

When the pre-processing options are set and applied to evidence as it is processed, in the case you can easily identify files that fit the criteria you set.

Filtering EID Material

The following tasks can help you use the EID feature.

Create an EID Tab Filter

A Tab Filter must be used here to filter the folders from the Explore tab, but not filter out the Folders' content from the Graphics Tab. However, the filter itself must be created first, then the filter must be applied as a Tab Filter.

To create a filter for the EID folders in your case

1. Click the **Explore** tab.
2. Ensure that Filters are turned off, and the Filter drop-down displays "-unfiltered-".
3. On the Menu bar, click **Filter >New**.
4. Create a Filter to include EID Folders that have high scores.
   4a. Give the Filter a name that reflects its purpose.
   4b. Provide a description with enough information to be helpful at a glance.
   4c. Set up rules. Check each rule to include it in the filter.
   4d. Mark **Live Preview** to see the effects of the filter on the current File List.
   4e. Choose **Match Any**, or **Match All**, to fit your needs, according to the preview.
   4f. Click **Save** > **Close**.
   If you choose to, repeat Steps 3 and 4 for Medium folders with a criteria of 40, then move to Step 5.
5. From the Filter Manager, copy the new filters to the **Include** list on the top-right side of the view.
6. At the bottom of the dialog, click **Apply** and **Close**.

To apply the new filter as a Tab filter

1. Click the **Explore** tab.
2. Ensure that Filters are turned off, and the Filter drop-down displays "-unfiltered-".
3. Click **Filter >Tab Filter**.
4. In the *Tab Filter Selection* dialog, click the drop-down to select **Explicit images folder (high score)** as created earlier.
5. Click **OK**.

Change the Column List Settings

To view the Explicit Image Detection (EID) statistics for your case in the File List, do the following:

1. Click the **Graphics** tab.
2. In the File List, select the default EID column template from the drop-down list, or add the EID columns to the column template you choose. To customize a Columns Template for EID content, do the following:
   2a. Click **Column Settings** in the File List toolbar.
   2b. In the *Manage Column Settings* dialog, click **New**, or highlight an existing template and click **Copy Selected**.
   2c. In the *Column Settings* dialog, select the EID-related column headings to add to the template, and click **Add**
   2d. Make your selections.
   2e. Move the selected columns up in the list to make them display closer to the left-most column in the view, as it best works for you.
3. Click **OK**
4. From the Manage Column Settings, select the New Column template, and click **Apply**.
   Later, to re-apply this column template, select it from the **Column Setting** drop-down.
   The resulting columns are displayed in the File List view
5. In the File List view, arrange the column headings so you can see the EID data.
6. Click any column heading to sort on that column, to more easily see and evaluate the relevant data.

EID Scoring

Each folder is given a score that indicates the percentage of files within the folder that have an EID score above 50. For example, if the folder contains 8 files and three of them score over 50, the folder score will be 38 (3 is 37.5% of 8). Now, a folder score of 38 does not mean there is no objectionable material in that folder, it only means that there is not a high concentration of objectionable material found there.

Explicit Image Detection filtering rates pictures according to the presence or absence of skin tones in graphic files. In addition, it not only looks for flesh tone colors, but it has been trained on a library of approximately 30,000 pornographic images. It assesses actual visual content. This capability increases the speed with which investigators can handle cases that involve pornography.

Successfully filtered pictures are issued a score between 0 and 100 (0 being complete absence of skin tones, and 100 being heavy presence of skin tones). A score above 100 indicates that no detection could be made. When you set filters for analyzing the scored data, you specify your own acceptance threshold limit for images you may consider inappropriate. Negative scores indicate a black and white, or grayscale image where no determination can be made, or that some error occurred in processing the file.

Descriptions of EID Scoring Values

0 to 100	The amount of skin tones detected. 0 = few skin tones detected, 100 heavy skin tones detected
-1	File not found
-2	License error

Descriptions of EID Scoring Values

-3	Wrong file format
-4	No match found
-5	Folder not found
-6	Unknown error
-7	Cannot load image (e.g., corrupt image)
-8	Not enough information
-9	Face detection profile path is null
-10	Can’t open face detection directory
-11	Face detection file not found
-12	Input classifier not initialized
-13	Init profile failed
-14	File path is empty
-16	Image data is empty
-17	Null matching handle
-18	Missing retrieval result
-100	An unsupported file format
-101	An unsupported black & white image
-102	An unsupported grayscale image
-103	An unsupported monochrome image
-1000	An unknown error
-1001	The EID score function threw an exception
-1002	The EID score function threw an exception

Using PhotoDNA to Compare Images

About Using PhotoDNA

You can use PhotoDNA to compare digital images against known contraband images so that you can quickly identify any contraband images in your evidence.

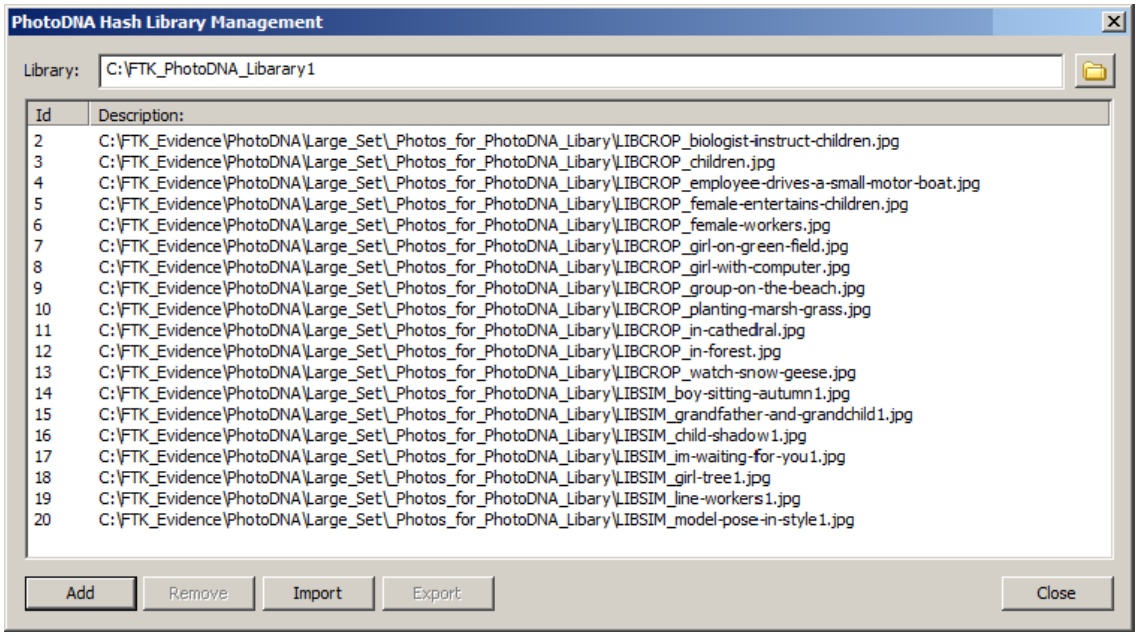
About the PhotoDNA Library Management Page

The PhotoDNA Library Management page is where you manage PhotoDNA libraries. From the PhotoDNA Management page, you can do the following:

- Specify the folder to be used for the library
- Add to or remove images from the library
- Edit the description of the photo in the library
- Import or export the library in order to share with others.

When an image file is added, PhotoDNA is run to analyze the file. A new row is created and an ID number is given to each photo. A description field displays the name of the photo. This description is an editable text field. You can add additional information to the description.

When you export, you can export all of the photos in a library or only one or more.



About the PhotoDNA Processing Option

You enable PhotoDNA for a case as a processing option. You can enable it at one of the following situations:

- When you create a new case

- When you add evidence to a case
- When you perform Additional Analysis

Enabling PhotoDNA will add time to processing. You can choose when to spend the extra time.

In the processing options, there is a PhotoDNA check box that is disabled by default. When you select the PhotoDNA check box, the PhotoDNA Library Management page is opened. You can select the location for an existing library or configure a new one.

When you enable PhotoDNA, the following occurs during evidence processing:

- A PhotoDNA value is generated for each image in the library.
- A PhotoDNA value is generated for each image in the evidence.
- The values for the images in the evidence is compared to the values in the library.
- A PhotoDNA score is generated for each image in the evidence.

You can view the score to see how similar images are to your library.

About viewing the PhotoDNA results

During processing, discovered images are analyzed by PhotoDNA and are given a DNA value. That image's DNA value is then compared to the DNA value in the PhotoDNA Library. A *PhotoDNA Distance* value is generated that represents how closely it matches any of the files in the library. (If the image matches more than one item in the library, the closest score is used).

The *PhotoDNA Distance* value can range from 0 to 49,000. A value of 0 means that there is no distance and the photo is a perfect match. Any score higher than the range means that there is no match and therefore no value is given.

After you have processed your evidence with PhotoDNA enabled, you can use the following three columns in the File List to display PhotoDNA information:

- PhotoDNA Data - Displays the description of the file in the library that the image most closely resembles. (By default, this is the path and filename of the photo in the library, but because the description is editable in the PhotoDNA Library Management interface, this will display whatever is in the description field.)
- PhotoDNA Difference - Displays the number indicating how closely the image matches a PhotoDNA library file (0 is a perfect match)
- PhotoDNA File ID - Displays the ID number of the file in the library as represented in the PhotoDNA Library Management interface.
- PhotoDNA Hash - The value of the PhotoDNA hash for the image.

See Comparing Images to the PhotoDNA Library on page 324.

Configuring a PhotoDNA Library

You configure a PhotoDNA library from the PhotoDNA Library Management page. You can do this at one of the following times:

- Outside of a case, from the Case Manager > Manage menu.
- Within a case when configuring Processing Options.

To configure a PhotoDNA Library

1. Open the PhotoDNA Library Management page by doing one of the following:
   - From the Case Manager, click Manage > PhotoDNA.
   - From within a case access the Processing Options.
2. Select a PhotoDNA Library by browsing to a folder location.

   If you have not previously created a library, specify a new folder location.

   If you have previously created a library, you can use it or create a new one.

   If you are in the Processing Options and it displays an existing library and you want to use a different one, clear the PhotoDNA option and re-select it.
3. To add photos to the library, do the following:

   3a. Click **Add**.

   3b. Browse to the photos that you want to add to the library.

   3c. Select the files that you want to add.

   3d. Click **Open**.
4. To remove photos from the library, select an item and click **Remove**.
5. Edit the description of an item, do the following:

   5a. Double-click an item.

   5b. Edit the description.

   5c. Click **OK.**
6. To export the library, do the following:

   6a. Select the photos that you want to export.

   6a. Click **Export**.

   6b. Specify a location to save the exported file.

   6c. Click **Save**.
7. To import a library, do the following:

   7a. Click **Import**.

   7b. Browse to an exported file.

   7c. Click **Import**.

   7d. Click **Save**.

Comparing Images to the PhotoDNA Library

You can compare the images in your case to the files in the PhotoDNA Library. The comparison is done during evidence processing. A PhotoDNA score is generated. You can view the score to see how similar images are to you library.

If you have an image in your evidence that you want to add to the PhotoDNA Library, you can do so with a right-click option.

You can perform a processing job at one of the following situations:

- When you add evidence to a case
- When you perform Additional Analysis

To compare images to the PhotoDNA Library

1. Either add evidence to a case or perform an Additional Analysis.
2. In the processing options, select the *PhotoDNA* check box.
3. Configure the PhotoDNA Library.
4. Click **OK**.

   Any images that are in the evidence will be processed, given a DNA value, and then compared against the files in the library.

To view the PhotoDNA scores

1. In the Examiner, use the *Overview* tab or the *Graphics* tab to view the graphics in your case.

   See Using the Graphics Tab on page 315.
2. Add columns to the File List that display the PhotoDNA score by doing the following:

   2a. Click the *Column Settings* icon.

   2b. Either create or edit a column settings template.

   2c. In the Available Columns list, expand *All Features*.

   2d. Select and *Add* the following columns:

   - PhotoDNA Distance - The value that shows how closely it matches a file in your library. For convenience, have this higher in the list than the other two.
   - PhotoDNA Data - The name of the file in the library that the image was compared to.
   - PhotoDNA File ID - The file ID of the file in the library that the image was compared to. (This ID is shown in the Photo ID Library Manager.

     See About viewing the PhotoDNA results on page 323.

   2e. Click **OK**.

   2f. Select the desired settings and click **Apply**.

   2g. You can sort by the PhotoDNA Distance value to see the photos that have the lowest scores and are the most likely matches.

To add images in the File List to the PhotoDNA library

❖ You can right-click a image file in the *File List* and click **Add to PhotoDNA library**.

The file is automatically added to the library. You can either remove it or click **Close.**

Chapter 23
Examining Videos

The *Video* tab lets you view detailed information about the video files in your cases.

You can generate thumbnails from video files and display them in the *Video Thumbnail* pane. This functionality lets you quickly examine a portion of the contents within video files without having to watch each media file individually.

See Generating Thumbnails for Video Files (page 327)

The *Video* tab also includes an embedded media player that lets you view the contents of video files. When you process the evidence in your case, you can choose to create a common video type for each of the various videos in your case. These common video types are not the actual video files from the evidence, but a copied conversion of the media that is generated by AccessData. These features let you view the contents of multiple video types, in a common resolution, and sampling rate, from within the *Examiner's* embedded media player.

See Creating Common Video Files (page 328)

When you process evidence, video thumbnails are created by default. To disable the creation of video thumbnails, turn off the *Create Thumbnails for Videos* option in the *Evidence Processing* options.

See Evidence Processing Options on page 82.

Generating Thumbnails for Video Files

You can generate thumbnail graphics based on the content that exists within video files in your case. Video thumbnail generation is accomplished during processing. You can either set up video thumbnail generation when you create a new case, or you can run the processing against an existing case by using the *Additional Analysis* dialog.

To generate thumbnails for video files

1. Do one of the following:
   - In the *Case Manager*, click **Case > New**. Then, click **Detailed Options**.
   - In the *Examiner*, click **Evidence > Additional Analysis > Hashing/Job Options**.
2. Check **Create Thumbnails for Videos**.
3. Click **Thumbnail Options**.
4. In the *Video Thumbnail Options* dialog, set from the following:

Percent	This option generates thumbnails against videos based on the percentage of a videos total content. For example if you set this value to 5, then at every 5% of the video a thumbnail is generated.
Interval	This option generates thumbnails against videos based on seconds. For example, if you set this value to 5, then at every 5 seconds within a video, a thumbnail is generated.

5. Click **OK**.

Generating Video Thumbnails from the Natural Viewer

You can also capture video thumbnails directly from a video viewed in the *Natural Viewer*. This feature allows you to find and capture specific information from video you are reviewing. After capturing a video thumbnail, you can then bookmark that thumbnail for future review.

To capture a video thumbnail from the Natural Viewer

1. From *Evidence Explorer*, click the *Video* tab.
2. Highlight the video and click the *Natural* tab in the *File Content* pane.
3. Click the **Play** button ( ).
4. Click the **Pause** button when you are ready to capture a video thumbnail.

   Note: You can navigate through the video using the Rewind and Fast Forward

5. Click **Add** in the bottom right corner of the *Video Thumbnails* pane.

   The application creates a video thumbnail of the paused frame and places that thumbnail in the *Video Thumbnail* pane.

Creating Common Video Files

When you process the evidence in your case or during Additional Analysis, you can choose to create a common video type for videos in your case. These common video types are not the actual video files from the evidence, but a copied conversion of the media that is generated and saved as an MP4 file that can be previewed on the video tab.

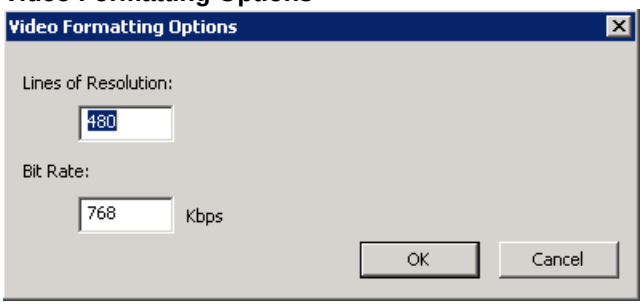
Common video files are not created by default.

See Evidence Processing Options on page 82.

To create common video files

1. Do one of the following:
   - In the *Case Manager*, Click **Case > New**. Then, click **Detailed Options**.
   - In the *Examiner*, click **Evidence > Additional Analysis**.
2. Check **Create Common Video Files**.
3. Process or analyze evidence.

Video Formatting Options



4. In the *Video Formatting Options* dialog, set the following:
   - **Lines of Resolution**: Sets the number of vertical lines in the video. The higher it is, the better the resolution.
   - **Bit Rate**: Sets the rate of bits in Kbps measurements. The higher it is, the better the resolution.
5. Click **OK**.

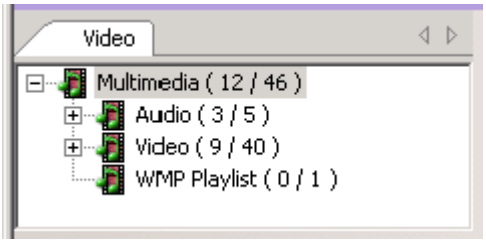
Using the Video Tree Pane

The *Video* tree pane lets you see the multimedia content in a tree view. The content that is displayed in the Video tab is dependent on a default *Tab Filter* called Video *Tab Filter: Video Thumbnails*.

The contents in the *Video* tree displays the multimedia contents in your case and information about the content that applies to the requirements of the Tab filter.

For example, in the graphic below, you can see that the case has 46 total multimedia files. 12 of those multimedia files meet the requirements of the Tab filter and therefore have had video thumbnails generated for them.

Video Tab: Video Tree Pane

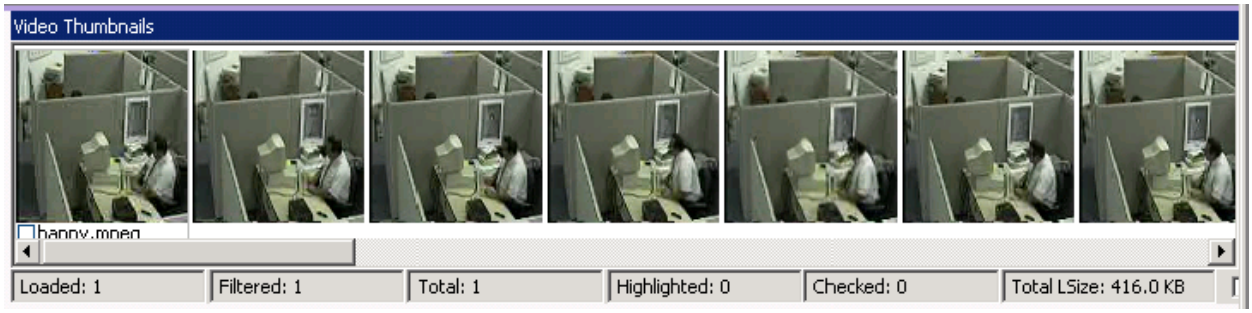


You can use the *Video* tree pane to navigate and drill down to specific multimedia containers and files. If you select a file in the tree pane, The Video Thumbnails pane and the File List pane display the content that is contained in your selection.

Using the Video Thumbnails Pane

The *Video Thumbnails* pane displays any video thumbnails that you have generated based on your selection in either the *Video* tree view or in the *File List* Pane.

Video Tab: Video Thumbnail Pane



You can use the *Video Thumbnail* pane to rapidly scan through the visual contents in a video file, without having to launch and watch the entire video.

In the *Video Thumbnails* pane, if a thumbnail could not be generated the following icon is displayed:

In the *Video Thumbnails* pane, beneath the first thumbnail image for a set of videos is a check box. You can select this check box to check the video file in the *Examiner*.

Playing a Video from a Video Thumbnail

You can play a video in the *File Content Viewer* starting from a selection in the *Video Thumbnail* pane.

For example, if you visually scan the contents of the video thumbnails pane and discover something you need to investigate in the *File Content* viewer, rather than watching the entirety of the video, you can select the location you want to start the video by selecting that thumbnail.

To Play a Video from the Location of a Video Thumbnail

1. In the *Video Thumbnails* pane, click the thumbnail from which you want to start the video.
2. In the *File Content Pane*, In the *Natural* tab, click the **Play** icon.
   The video begins to play from the location that you selected in the *Video Thumbnails* pane.

The Thumbnail Size Setting

You can change the size of the thumbnails that are displayed in the Video tab of the Examiner.

See The Thumbnails Size Setting (page 316) for information on how to do this.

Moving the Thumbnails Pane

You can move, float, and dock the thumbnails pane in the Video tab of the Examiner.

See Moving the Thumbnails Pane (page 317) for information on how to do this.

Chapter 24
Examining Miscellaneous Evidence

This chapter contains information on the following ways to view evidence:

- Identifying Processing-Generated Data (page 333)
- Relating Generated Files to Original Files (page 333)
- Viewing Windows Prefetch Data (page 334)
- Viewing Data in Windows XML Event Log (EVTX) Files (page 334)
- Viewing IIS Log File Data (page 336)
- Viewing Registry Timeline Data (page 338)
- Viewing Log2Timeline CSV File Data (page 340)
- Identifying Document Languages (page 343)
- Examining Internet Artifact Data (page 345)
- Examining Mobile Phone Data (page 352)
- Viewing Data in Volume Shadow Copies (page 361)
- Viewing Microsoft Office and Adobe Metadata (page 361)

Identifying Processing-Generated Data

There are some files that get generated during processing. Examples of these files include data broken out from compound files, EXIF data from images, file metadata, and so on. There is a column called Actual File which can be used in the File List to designate if the file was in the original data (True) or if it was generated during processing (False).

See Managing Columns on page 480.

Also, when looking at the file name at the bottom of the File List, if the file was generated by FTK, there is an >> after the parent file name and before the generated file name.

For example, photo.jpg>>photo.exif.html, or mystuff.zip>>pass.doc

See File List Pane on page 301.

You can also use bookmarks to relate generated files with the actual source file in the evidence.

See Identifying Processing-Generated Data on page 333.

Relating Generated Files to Original Files

Some files in your evidence may not be original files but may have been generated during processing. Examples of these files include data broken out from compound files, EXIF data from images, file metadata, and so on.

You can use bookmarks to quickly relate generated files with the actual source filed in the evidence. By selecting the *Actual Source File* option, the source file will be listed and bookmarked as well. All parent items are recursively related within the bookmark from the generated item to the actual source file and not just a parent folder.

See Creating a Bookmark on page 372.

For example, during processing, a DOC file may be generated from a ZIP file. If you bookmark the DOC file and select the *Actual Source File* option, the original ZIP file is included in the bookmark as well.

The related items are also shown in the bookmark section of reports.

You can also view information in the File List to identify processing-generated files.

See Identifying Processing-Generated Data on page 333.

To relate generated files to the original files in bookmarks

1. Right-click a file that was generated during processing.
2. Click either **Create Bookmark** or **Add to Bookmark**.
3. On the bookmark dialog, select *Actual Source File*.

Viewing Windows Prefetch Data

You can easily view data about Windows prefetch (PF) files. When you select a prefetch file in the *File List*, the following application data is displayed in HTML format in the *Natural* tab of the *File Content* pane:

- The file path of the application executable file
- The number of times the application has been run
- The last time the application was run

Viewing Data in Windows XML Event Log (EVTX) Files

About Viewing EVTX Log Files

You can view Microsoft Windows XML event log data. You can view event data in HTML format in the *Natural* tab of the *File Content* pane.

You can view event data in one of two ways:

View event data that is contained in Microsoft Windows XML event log (EVTX) files	In the *File List*, you can see a list of all of the EVTX files. When you view an EVTX log file, in the *File Content* pane, you can view the information about all of the events that are contained in that one file. There can be a lot of data contained in one file.
Expand EVTX log files into separate objects for every event record	When you expand EVTX log files, each event is extracted as its own record. As a result, in the *File List*, each event is shown as its own item. Each item has a small amount of data in it but there can be many individual event records. For example, you may have 100 EVTX log files, and if you expand them, you can have over 100,000 individual event records. When you process evidence, you have the option of expanding EVTX log files. The options is turned off by default. See Evidence Processing Options on page 99. See Using Additional Analysis on page 151. If you expand EVTX files into separate event objects, you can also use the following columns in the *File List*: • EVTX Event Channel • EVTX Event Computer • EVTX Event Data • EVTX Event ID • EVTX Event Level • EVTX Event Source • EVTX Event Source Name • EVTX Event User ID

If you expand data, you will have files are are generated when the data was processed and was not part of the original data. There are tools to help you identify generated data.

See Identifying Processing-Generated Data on page 333.

See Relating Generated Files to Original Files on page 333.

To view EVTX log files

1. In the Examiner, click **Overview**.
2. In *Case Overview*, do one of the following:
   - View by file extension:
     - Click **File Extension**.
     - If present, click **evtx**.
   - View by file category:
     - Click **File Category**.
     - If present, click **Windows EVTX Event Log**.
3. If your case has any EVTX files, they are displayed in the *File List*.
4. Click an EVTX file to view the data in the *Natural* tab.
   Some log files may not contain any events and you will only see the heading *EVTX Events*.

To expand EVTX log files into individual event records

1. In the Examiner, click **Evidence > Additional Analysis**.
   See Using Additional Analysis on page 151.
2. Under *Miscellany*, select **Expand Compound Files**.
3. Click **Expansion Options**.
4. Select **EVTX**.
5. Click **OK** to save the expansion settings.
6. Click **OK** to process the evidence to expand EVTX files.

To view individual event records

1. In the Examiner, click **Overview**.
2. In *Case Overview*, Click **File Category**.
3. If present, click **Windows EVTX Event**.
4. If your case has any event records, they are displayed in the *File List*.
5. Click an event record to view the data in the *Natural* tab.

To add EVTX-related columns in the File List

❖ To add EVTX-related columns in the *File List*, add the EVTX-related columns to a new or existing column template.

See Managing Columns on page 480.

These columns will display data only for the expanded individual events, not for the EVTX log files.

Viewing IIS Log File Data

You can view data that is contained in IIS log files in HTML format in the *Natural* tab of the File Contents Pane.

You can also process IIS log files so that they are broken into individual records and interspersed with other items to support timeline analysis. To process IIS log files, there is a new *IIS LOG* check box in *Evidence Processing Options* > *Expansion Options*. This option is not enabled by default.

You can view IIS log data in one of two ways:

View the log file data	In the *File List*, you can see a list of IIS log files. When you view a log file, in the *File Content* pane, you can view the information that are contained in that one file. There can be a lot of data contained in one file.
Expand log file data out as individual records	When you expand IIS log files, each record is extracted. As a result, in the *File List*, each record is shown as its own item. When you process evidence, you have the option of expanding IIS log files. The options is turned off by default. See Evidence Processing Options on page 99. See Using Additional Analysis on page 151. If you expand IIS log files into separate records, you can also use the following columns in the *File List*: ● c-ip ● cs(Cookie) ● cs(Referer) ● cs(User-Agent) ● cs-bytes ● cs-host ● cs-method ● cs-uri-query ● cs-uri-stem ● cs-username ● s-computername ● s-ip ● s-port ● s-sitename ● sc-bytes ● sc-status

If you expand data, you will have files are are generated when the data was processed and was not part of the original data. There are tools to help you identify generated data.

See Identifying Processing-Generated Data on page 333.

See Relating Generated Files to Original Files on page 333.

To expand IIS log files into individual records

1. In the Examiner, click **Evidence > Additional Analysis**.

   See Using Additional Analysis on page 151.
2. Under *Miscellany*, select **Expand Compound Files**.
3. Click **Expansion Options**.
4. Select **IIS Log**.
5. Click **OK** to save the expansion settings.
6. Click **OK** to process the evidence to expand the files.

To add IIS log-related columns in the File List

- To add IIS log-related columns in the File List, add the IIS log-related columns to a new or existing column template.

  See Managing Columns on page 480.

  These columns will display data only for the expanded individual records, not for the IIS log files.

Viewing Registry Timeline Data

You can view registry additional data in HTML format in the *Natural* tab of the *File Contents Pane* to support timeline analysis.

You can process Registry data files so that they are broken into individual records so they are interspersed with other items to support timeline analysis. To process Registry data, there is a new *Registry* check box in *Evidence Processing Options* > *Expansion Options*. This option is not enabled by default.

The following registry areas are supported:

- SAM:
  - SAM\Domains\Account\Users
- NTUSER.DAT:
  - Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count
  - Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count
  - Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count
  - Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}\Count
  - Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\CIDSizeMRU
  - Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\FirstFolder
  - Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU
  - Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRULegacy
  - Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU

You can view Registry data in one of two ways:

View the Registry data	In the *File List*, you can view Registry files.
Expand Registry data out as individual records	When you expand Registry data, each record is extracted. As a result, in the *File List*, each record is shown as its own item. When you process evidence, you have the option of expanding Registry data. The options is turned off by default. See Evidence Processing Options on page 99. See Using Additional Analysis on page 151. If you expand Registry data into separate records, you can also use the following columns in the *File List*: • Registry Action Description • Registry Action Name • Registry Action Type • Registry File

If you expand data, you will have files are are generated when the data was processed and was not part of the original data. There are tools to help you identify generated data.

See Identifying Processing-Generated Data on page 333.

See Relating Generated Files to Original Files on page 333.

To expand Registry data into individual records

1. In the Examiner, click **Evidence > Additional Analysis**.
   See Using Additional Analysis on page 151.
2. Under *Miscellany*, select **Expand Compound Files**.
3. Click **Expansion Options**.
4. Select **Registry**.
5. Click **OK** to save the expansion settings.
6. Click **OK** to process the evidence to expand the files.

To add Registry-related columns in the File List

- To add Registry-related columns in the File List, add the Registry-related columns to a new or existing column template.
  See Managing Columns on page 480.

These columns will display data only for the expanded individual records.

Viewing Log2Timeline CSV File Data

You can view data that is contained in CSV files that are in the Log2timeline format. You can view the data in the *Natural* view of the *File Content* pane.

The individual records from the CSV will be interspersed with other data, giving you the ability to perform more advanced timeline analysis across a very broad set of data. In addition you can leverage the visualization engine to perform more advanced timeline based visual analysis.

To process CSV files, there is a new *Log2tCSV* check box in *Evidence Processing Options* > *Expansion Options*. This option is not enabled by default.

You can view CSV data in one of two ways:

View the original CSV files	In the *File List*, you can see a list CSV files. When you select a file, you can view the information that is contained in each file in the *File Content* pane .
Expand log file data out as individual records	When you expand CSV files, each record is extracted. As a result, in the *File List*, each record is shown as its own item. When you process evidence, you have the option of expanding CSV files. The options is turned off by default. See Evidence Processing Options on page 99. See Using Additional Analysis on page 151. If you expand CSV files into separate records, you can also use columns to view each CSV field. See the table Log2timeline CSV fields (page 342)

If you expand data, you will have files are are generated when the data was processed and was not part of the original data. There are tools to help you identify generated data.

See Identifying Processing-Generated Data on page 333.

See Relating Generated Files to Original Files on page 333.

To view the un-expanded CSV files

1. In the Examiner, click the **Overview** tab.
2. Expand **File Category.**
3. If CSV files exist in your evidence, you can expand **Other Known Types** > **Log2t CSV logs**.
   A list of Log2t CSV files is displayed in the *File List*.
4. Click a file to view the un-expanded data.

To expand CSV files into individual records

1. In the Examiner, click **Evidence > Additional Analysis**.
   See Using Additional Analysis on page 151.
2. Click **Miscellaneous**
3. Under *Miscellany*, select **Expand Compound Files**.
4. Select **Expand Compound Files**.

5. Click **Expansion Options**.
6. Select **Log2t CSV**.
7. Click **OK** to save the expansion settings.
8. Click **OK** to process the evidence to expand the files.

To add CSV-related columns in the File List

1. In the Examiner, click the Column Settings icon.
   See Managing Columns on page 480.
2. Either create a new column template or edit an existing one.
3. In the **Available Columns** list, expand **Log2T**.
4. Add the desired columns to the template.
5. Click **OK.**
6. Select the template name you just configured.
7. Click **Apply.**
   This applies the template to the File List.
8. Click **Close.**
9. In the Overview tab, expand **File Category** > **Other Known Types** > **Log2t CSV log entry**.
   A list of Log2t entries is displayed in the *File List*.
   You will see the data in the columns for each record.
   These columns will display data only for the expanded individual records, not for the original CSV files.

Log2timeline CSV fields

Log2t Desc	A description field, this is where most of the information is stored. This field is the full description of the field, the interpreted results or the content of the actual log line..
Log2t Extra	Additional information parsed is joined together and put here. This 'extra' field may contain various information that further describe the event. Some input modules contain additional information about events, such as further divide the event into source IP's, etc. These fields may not fit directly into any other field in the CSV file and are thus combined into this 'extra' field.
Log2t Filename	The full path of the filename that contained the entry. In most input modules this is the name of the logfile or file being parsed, but in some cases it is a value extracted from it, in the instance of $MFT this field is populated as the name of the file in question, not the $MFT itself.
Log2t Format	The name of the input module that was used to parse the file. If this is a log2timeline input module that produced the output it should be of the format Log2t::input::NAME where name is the name of the module. However other tools that produce l2t_csv output may put their name here.
Log2t Host	The hostname associated with the entry, if one is available.
Log2t Inode	The inode number of the file being parsed, or in the case of $MFT parsing and possibly some other input modules the inode number of each file inside the $MFT file.
Log2t MACB	The MACB or legacy meaning of the fields, mostly for compatibility with the mactime format.
Log2t Notes	Some input modules insert additional information in the form of a note, which comes here. This might be some hints on analysis, indications that might be useful, etc. This field might also contain URL's that point to additional information, such as information about the meaning of events inside the EventLog, etc.
Log2t Short	The short description of the entry, usually contains less text than the full description field. This is created to assist with tools that try to visualize the event. In those output the short description is used as the default text, and further information or the full description can be seen by either hovering over the text or clicking on further details about the event.
Log2t Source	The short name for the source. This may be something like LOG, WEBHIST, REG, etc. This field name should correspond to the type field in the TLN output format and describes the nature of the log format on a high level (all log files are marked as LOG, all registry as REG, etc.)
Log2t SourceType	A more comprehensive description of the source. This field further describes the format, such as "Syslog" instead of simply "LOG", "NTUSER.DAT Registry" instead of "REG", etc.
Log2t User	The username associated with the entry, if one is available.
Log2t Version	The version number of the timestamp object.

Identifying Document Languages

When processing evidence, you can perform automatic language identification. This will analyze the first two pages of every document to identify the language that is contained within.

To identify languages, you enable the Language Identification processing option.

See Evidence Processing Options on page 99.

See Using Additional Analysis on page 151.

After processing is complete, you can add the *Language* column in the File List in the Examiner.

See Managing Columns on page 480.

You can filter by the Language field within review and determine who needs to review which documents based on the language contained within the document.

If there are multiple languages in a document, the first language will be identified.

This feature is enabled by selecting a new *Language Identification* processing option. When you enable Language Identification, you have the following options:

- Document Types to process - You can select to process the following file types:
  - Documents
  - Presentation
  - Spreadsheets
  - Email
- The languages to identify - You can select to identify the following:
  - Basic languages that include English, Chinese, Spanish, Japanese, Portuguese, Arabic, French, Russian, and Korean.
  - Extended languages. Performs language identification for 67 different languages. This is the slowest processing option.

Note: The Language Identification processing option is disabled by default. If you enable it, the basic language setting and all four document types are enabled by default.

Basic Languages

The system will perform language identification for the following languages:

- Arabic
- Chinese
- English
- French
- German
- Japanese
- Korean
- Portuguese
- Russian

- Spanish

If the language to identify is one of the ten basic languages (except for English), select Basic when choosing Language Identification. The Extended option also identifies the basic ten languages, but the processing time is significantly greater.

Extended Languages

The system will perform language identification for 67 different languages. This is the slowest processing option. The following languages can be identified:

• Afrikaans	• Esperanto	• Latin	• Scottish Gaelic
• Albanian	• Estonian	• Latvian	• Serbian
• Amharic	• Finnish	• Lithuanian	• Slovak
• Arabic	• French	• Malay	• Slovenian
• Armenian	• Georgian	• Manx	• Spanish
• Basque	• German	• Marathi	• Swahili
• Belarusian	• Greek	• Nepali	• Swedish
• Bosnian	• Hawaiian	• Norwegian	• Tagalong
• Breton	• Hebrew	• Persian	• Tamil
• Bulgarian	• Hindi	• Polish	• Thai
• Catalan	• Hungarian	• Portuguese	• Turkish
• Chinese	• Icelandic	• Quechua	• Ukrainian
• Croatian	• Indonesian	• Romanian	• Vietnamese
• Czech	• Irish	• Rumantsch	• Welsh
• Danish	• Italian	• Russian	• Yiddish
• Dutch	• Japanese	• Sanskrit	• West Frisian
• English	• Korean	• Scots	

Examining Internet Artifact Data

You can examine detailed information about the internet artifact data in your case.

At a basic level, when evidence is processed, internet artifact files are categorized and organized so that you can easily see them. You can use either of the following to quickly see internet artifact files:

- The *Overview* tab > *File Category* > *Internet/Chat Files*
- The *Internet/Chat* tab

Both tabs display the same data.

For example, using these views, you can quickly see the following files:

- AOL:
  - AOL ABY files
  - AOL Buddy List
  - AOL User History
- Chrome Browser:
  - Bookmark files
  - Cookies files
  - History files
- Internet Explorer:
  - MSIE Cookie Index files
  - MSIE History files
- Microsoft Live Messenger Log files
- Mozilla
  - Address Book files
  - Cookie Index files
  - History files
  - Mozilla Thunderbird email files
- Skype
  - Skype Data
  - Skype Files
- Web-based email providers
  - Flashmail
  - Foxmail
- Yahoo IM conversation files
- mail.ru agent history files (Mra.dbs):
  - User account information and encrypted account password
    From the registry at HKCU\Software\Mail.Ru\Agent\magent_logins3*\
  - Parsed contacts and messages from mra.dbs files
    Each message contains a plain-text and an RTF version, both UTF16LE.
  - Contact list from the inbox.ru.xml.

For many of these files, you can view information from the files in the Natural view. For example, you can see an AOL Buddy List or the contents of a Yahoo IM conversation.

Some internet artifact information is stored in SQLite tables. Most of these tables are viewable in the Natural view.

About Extensible Storage Engine (ESE) Databases

Extensible Storage Engine (ESE) databases are used by many Microsoft components as well as other programs to store and retrieve data. Some of these components include:

- MS Exchange Server (2000/2003)
- MS Exchange Server (2007)
- MS Exchange Server (2010)
- Active Directory
- Windows Live Server
- Desktop Search (Vista and Windows 7)
- IE 10 Web Data (for example, history, cookies, cache, and so forth)
- SRS (Site Replication Service) Template
- Windows Help Center
- Windows Update
- Windows System Update
- Windows Server Security
- Windows Server WINS
- Windows Server DHCP
- NT File Replication Service

These ESE databases are expanded when processing evidence (if selected in the Expansion Options) and displayed in Evidence Groups. Most of the ESE databases appear in *File Category* > *Databases*. The exception is Exchange ESE databases, which appear in *File Category* > *Email*.

Internet Explorer version 10 or later also use ESE databases to store data like the internet history, cookies, cache, and so forth. (See About Expanding Data from Internet Explorer (IE) Version 10 or Later on page 348.)

To expand the ESE Databases into individual records

1. In the Examiner, click **Evidence > Additional Analysis**.
   See Using Additional Analysis on page 151.
2. Click **Miscellaneous**
3. Under *Miscellany*, select **Expand Compound Files**.
4. Select **Expand Compound Files**.
5. Click **Expansion Options**.
6. Verify that **ESE DB** is selected.
7. Click **OK** to save the expansion settings.
8. Click **OK** to process the evidence to expand the files.

About Expanding Google Chrome, Firefox, and IE 9 Data

There are advanced processing options that will expand the basic Google Chrome, Mozilla Firefox, and Internet Explorer data. You can do the following:

- Expand Google Chrome and Mozilla Firefox SQLite tables and IE 9 IE.DAT files to create individual records.

  This provides investigators the ability to bookmark specific records from within the tables. For example, if you are looking for a specific Top Site record, you can more easily find and bookmark the record you need.

- Reconstruct web pages .

  When viewing either Cache or History entries, if enough data is stored in the cache, you can see the reconstructed web page that was cached when the user was browsing the respective web site.

The following table lists the expanded data that you can view:

Internet Artifact Expanded Data

Chrome	• Cache Index Data • Cookies • Downloads • History • Top Sites • Key Words • Web Autofill Data
Firefox	• Bookmarks • Cache Index Data • Cookies • Favorites • Form History • History
Internet Explorer 9	• IE Cache Entries • IE Cookies Entries • IE History Entries • IE Download Entries • MSIE Recovery dat Entries

When viewing the expanded data, you can use the following columns in the File List to display detailed data.

Internet History Columns

- Action URL
- Autofill Name
- Autofill Value
- Bytes Downloaded
- Cookie Name
- Cookie Path
- Cookie Value
- Count
- Duration
- Encrypted Card Number
- End Time
- Expiration Month
- Expiration Time
- Expiration Year
- File Path
- Google Profile Address
- Google Profile City
- Google Profile Company Name
- Google Profile Country
- Google Profile Country Code
- Google Profile Email Address
- Google Profile First Name
- Google Profile Last Name
- Google Profile Middle Name
- Google Profile Phone Number
- Google Profile State
- Host Key
- Last Updated Time
- Last Visit Time
- Name on Card
- Offline User Email
- Opened
- Origin URL
- Password Element
- Password Value
- Rank
- Redirects to
- Start TIme
- Terms
- This Visit Time
- Types Times
- URL
- URL has HTML
- Username Element
- Username Value
- Visit TImes
- Zip Code

See Managing Columns on page 480.

See Icons of the File List Tool Bar on page 303.

If you expand internet artifact data, you will have files are are generated when the data was processed and was not part of the original data. There are tools to help you identify generated data.

See Identifying Processing-Generated Data on page 333.

See Relating Generated Files to Original Files on page 333.

About Expanding Data from Internet Explorer (IE) Version 10 or Later

Data from Internet Explorer (IE) 10 is stored in a database called WebCacheV01.dat. This file is an ESE (Extensible Storage Engine) database that points to IE 10's cached files. When expanded in Examiner, you can view the following data:

Internet Artifact Expanded Data

Internet Explorer 10	• IE Web Cache Compatibility Entries • IE Web Cache Content Entries • IE Web Cache Cookie Entries • IE Web Cache DOM Store Entries • IE Web Cache Download Entries • IE Web Cache RSS Feed Entries • IE Web Cache History Entries • Other Web Cache Entries

This data displays in the Overview tab under Internet/Chat Files or in the Internet/Chat tab.

IE 10 (and later) WebCache Data on a Live System

You cannot expand or display Internet Explorer 10 (or later) WebCache data from a live system. WebCache data is locked by the Windows operating system and does not display correctly in the Examiner.

About Internet Artifact Processing Options

To expand internet artifact data, you enable processing options either when you add the evidence or later by using Additional Analysis.

Note: The IE WebCache contains many files and can take additional time to expand. Therefore, IE WebCache is not selected by default.

Important: Expanding internet artifact data can add a significant amount of data to your evidence.

See Evidence Processing Options on page 99.

See Using Additional Analysis on page 151.

Internet Artifact Processing Options

Chrome	Expand Compound Files > Chrome Bookmarks	unselected by default
	Expand Compound Files > Chrome Cache	unselected by default
	Expand Compound Files > Chrome SQLite	unselected by default
Firefox	Expand Compound Files > Firefox Cache	unselected by default
	Expand Compound Files > Firefox SQLite	unselected by default
Internet Explorer 9 or earlier	Expand Compound Files > Internet Explorer	selected by default
	Expand Compound Files > IE Recovery This lets you expand *IE Recovery* data that was stored when access to a Web site was lost.	unselected by default
Internet Explorer 10 or later	Expand Compound Files > IE WebCache	unselected by default

About Viewing Internet Artifact Data

After you have expanded the artifact data, you can view the data in the Examiner. You can view expanded data in one of the following ways:

- Clicking an individual file and viewing the contents in the Natural view.
  For most items, you will see the data displayed in a table.
  - Viewing Reconstructed web pages
    For history and cache entries, if enough data exists, the reconstructed web page appears. If enough data is not available, informational data appears instead.
    You can use the *URL has HTML* column to help you determine which files can be reconstructed.

- Adding columns to the *File List* that displays expanded data.

  You can add columns for all of the expanded items that is generated. A sample is listed in the *Internet History Columns* table above.

  You can view a list of all of the Internet History columns by looking at the *Internet History* column group in the column manager.

  See Managing Columns on page 480.

In the Internet/Chat files folder, the files are organized as follows:

- Chrome:
  - Original Chrome artifact files are stored under the *Chrome Browser Files* folder
  - The expanded data is stored under the *Chrome Browser Data* folder.
- Firefox:
  - Original Firefox artifact files are stored under the *Firefox Files* folder
  - The expanded data is stored under the *Firefox Browser Data* folder.
- IE
  - Original IE artifact files are stored under the *Internet Explorer Browser Files* folder
  - The expanded data is stored under the *Internet Explo*rer *Browser Data* folder.

Expanding Internet Artifact Data

To expand internet artifact data

1. When either adding evidence to a case or performing Additional Analysis, access the processing options.

   See Evidence Processing Options on page 99.

   See Using Additional Analysis on page 151.
2. Select the option to **Expand Compound Files**.
3. Click **Expansion Options**.
4. Select one or more of the following options:
   - Chrome:
     - Chrome Bookmarks
     - Chrome Cache
     - Chrome SQLite
   - Firefox:
     - Firefox Cache
     - Firefox SQLite
   - IE:
     - IE Cookie Text
     - IE Recovery
     - IE WebCache
     - Internet Explorer Files
   - Skype SQLite

     See About Internet Artifact Processing Options on page 349.
5. Process your data.

Viewing Internet Artifact Data

To view expanded internet data in the Natural view

1. In the examiner, open one of the following: (Both tabs display the same data.)
   - The **Overview** tab > **File Category** > **Internet/Chat Files**

   Note: Chrome and Firefox SQLite files are also located in Internet/Chat Files.

   - The **Internet/Chat** tab
2. For Chrome files, expand **Chrome Browser** > **Chrome Browser Data**.
3. For Firefox files, expand **Mozilla Files > Firefox Browser > Firefox Browser Data**.
4. For IE files, expand **Internet Explorer Browser** > **Internet Explorer Browser Data**.
5. Select a folder, such as **Cookies**.
6. Click an item in the *File List*.
   The cookie's data is displayed in the *Natural* view.
7. Click **History**.
8. Click an item in the *File List*.
   If possible, the reconstructed web page will be shown. If insufficient data exists, informational data will be shown instead.
9. You can perform a search for a specific value in the Natural view by clicking CTRL-F.

To view expanded internet data using columns

1. In the examiner, open one of the following: (Both tabs display the same data.)
   - The **Overview** tab > **File Category** > **Internet/Chat Files**
   - The **Internet/Chat** tab
2. Click the *Column Settings* icon.
   See Managing Columns on page 480.
3. Either create a new column template or edit an existing one.
4. In the **Available Columns** list, expand **Data**.
5. Add the desired columns to the template.
   For example, to add columns for Chrome or Firefox browser history data, use the following:
   - URL
   - Visit TImes
   - Typed Times
   - Last VIsit Time
   - This Visit Time
   - Duration
6. Click **OK**.
7. Select the template name you just configured and click **Apply**.
   This applies the template to the *File List*.
8. Click **Close**.
9. Expand **Browser** > **Browser Data** for either Chrome or Firefox.
10. Click **History**.
    In this example, you will see the history data in the columns for each record.

Examining Mobile Phone Data

You can examine detailed information about the mobile phone data in your case.

The mobile phone data that you can see comes from the following sources:

- AD1 files from AccessData Mobile Phone Examiner
- Cellebrite UFDR report files
  See Working with Cellebrite UFDR Images on page 358.

At a basic level, when evidence is processed, mobile phone files are categorized and organized so that you can easily see them. You can use the *Overview* tab to quickly view data specific to mobile phones:

- The *Overview* tab > *File Category* > *Mobile Phone*

For example, using these views, you can quickly see the following files:

- *Mobile Phone Data*
  - *Bookmark*
  - *Call History*
  - *Cookie*
  - *Powering Event*
  - *SMS Messages*
  - *Web History*
- *Mobile Phone Files*
  - *Cellebrite Files*

For many of these files, you can view information from the files in the Natural view. For example, you can see artifacts for the Call History or the contents of an SMS Message.

Some mobile phone information is stored in SQLite tables. Most of these tables are viewable in the Natural view.

Note: The files listed in the *Mobile Phone Data* section are specific to the particular mobile phone image you have processed, and will be different for each mobile phone image.

There are many files found on mobile phones that are not specific to the Mobile Phone file category. This data could include, but is not limited to, the following file categories:

- Archives
- Databases
- Documents
- Folders
- Graphics

These files can also be viewed by using the *Overview* tab.

About Expanding Mobile Phone Data

When viewing the expanded mobile phone data, you can use the following columns in the File List to display detailed data.

Mobile Phone Columns	
App Usage	• App Activation Count • App Active Time • App Background Time • App Launch Count • App Launch Day • App Name
Bluetooth Device	• Bluetooth Device Info • Bluetooth Device MAC Address • Bluetooth Device Name
Calendar	• Calendar Priority • Event Category • Event Description • Event End Time • Event Location • Event Phone Number • Event Start Time • Event Status • Event Summary • Event Timezone • Reminder Timestamp
Call History	• Call Duration • Call Number • Call Time • Call Type • Calling Name • Country Code • Network Code • Network Name • Phone Call Type
Installed Apps	• App Category • App Description • App GUID • App Identifier • App Install Time • App Name • App Update Timestamp • App Vendor • App Version • Copyright • Permissions • Purchase Date

Mobile Phone Columns

IP Connection	• Cellular Wan • Connection Adapter • Connection IP Address • Connection Status • Connection Type • Device IPs • DNS Addresses • Domain • MAC Address • Router Address • Service Name
Location	• Elevation • Latitude • Location Address • Location Category • Location Confidence • Location Country • Location Description • Location Name • Location Type • Longitude • Precision
Miscellaneous File Info	• Folder Name • Group • Item Source • Local File Path • Related Account • Related Application • Related URL • Storage Location • Storage Type
MMS Messages	• MMS BCC • MMS CC • MMS File Count • MMS From • MMS Priority • MMS Received Timestamp • MMS Sent Timestamp • MMS Status • MMS Subject • MMS To
Mobile Card	• Card Activation Time • Card Barcode • Card Description • Card Expiration Time • Card Name • Card Purchase Time • Card Type

Mobile Phone Columns

Notification	• Notification ID • Notification Participants • Notification Status • Notification Subject • Notification To • Notification Type
Password	• Password Account • Password Data • Password Server • Password Service
Phone Info	• Dictionary Locale • Dictionary Word • Event Severity • Package Name • Participant • Participant Email • Powering Event • Powering Event Element • Process • Type

Mobile Phone Columns

Phonebook	• Address • Address Type • Address1 • Address2 • City • Company • Email • First Name • Home Address • Home Email • Home Number • Last Name • Last Time Contacted • Middle Name • Mobile Number • Nickname • Number Type • Personal Mobile Number • Phone Number • Phonebook Item Home Website • Phonebook Item Name • Phonebook Item URL • Phonebook Item Work Website • Phonebook Label • State • Times Contacted • Title • Work Address • Work Email • Work Mobile Number • Work Number • Zip
SMS Messages	• SMS From • SMS From Number • SMS Service Center • SMS State • SMS Text • SMS Time Received • SMS Time Sent • SMS Time Zone of Sender • SMS To • SMS To Number • SMS Type
VoiceMail	• VM Duration • VM From • VM Name

Mobile Phone Columns	
WiFi	• BSSID • Last Connected • Last Network • Network Protocol • SSID • Wireless Security Mode
Note Summary	
Note Title	
Task Time Zone	

Viewing Mobile Phone Data

To view expanded mobile phone data in the Natural view

1. In the examiner, open the following:
   - The **Overview** tab > **File Category** > **Mobile Phone** > **Mobile Phone Data**
2. Select a folder, such as **SMS Messages**.
3. Click an item in the *File List*.
   The data is displayed in the *Natural* view.
4. Click **Mobile Phone Files**.
5. Click **Extraction Summary** in the *File List*.
   Details of the original mobile phone extraction will be shown.
6. You can perform a search for a specific value in the Natural view by clicking CTRL-F.

To view expanded mobile phone data using columns

1. In the examiner, open the following:
   - The **Overview** tab > **File Category** > **Mobile Phone**
2. Click the Column Settings icon. There are six mobile phone templates available:
   - Mobile Device Apps
   - Mobile Device Call Log
   - Mobile Device Contacts
   - Mobile Device Events
   - Mobile Device MMS
   - Mobile Device SMS
3. Either create a new column template or edit an existing one.
   See Managing Columns on page 480.
4. In the **Available Columns** list, expand **Mobile Phones**.

5. Add the desired columns to the template.
   For example, to add columns for SMS Messages data, use the following:
   - SMS From
   - SMS From Number
   - SMS Service Center
   - SMS State
   - SMS Text
   - SMS Time Received
   - SMS Time Sent
   - SMS Time Zone of Sender
   - SMS To
   - SMS To Number
   - SMS Type
6. Click **OK**.
7. Select the template name you just configured and click **Apply**.
   This applies the template to the File List.
8. Click **Close**.
9. Apply the *Mobile Device SMS* column template.
10. Expand **Mobile Phone** > **Mobile Phone Data**.
11. Click **SMS Messages**.
    In this example, you will see the SMS data in the columns for each record.

To view expanded mobile phone data using filters

1. In the examiner, open the following:
   - The **Overview** tab > **File Category** > **Mobile Phone**
2. Click the *Filter* dropdown. There are five mobile phone templates available:
   - Mobile Phone: Calendar
   - Mobile Phone: Call History
   - Mobile Phone: Messages
   - Mobile Phone: Phonebook
   - Mobile Phone Files
3. Either apply an existing filter or create a new one.
   See Managing Filters on page 51.
4. Once applied, you will see only those items allowable by the selected filter. The *File List* contents will also be highlighted yellow, showing a filter is applied.

Working with Cellebrite UFDR Images

About Expanding Cellebrite Data

To expand Cellebrite mobile phone data, you enable processing options either when you add the evidence or later by using Additional Analysis.

See Evidence Processing Options on page 99.

See Using Additional Analysis on page 151.

Expanding Cellebrite Data

To expand Cellebrite data

1. When either adding evidence to a case or performing Additional Analysis, access the processing options.

   See Evidence Processing Options on page 99.

   See Using Additional Analysis on page 151.
2. Select the option to **Expand Compound Files**.
3. Click **Expansion Options**.
4. Click **Clear All**.
5. Select the **Cellebrite UFDR** option.
6. Process your data.

Working with iOS Backup

About Expanding iOS Backup Data

To expand iOS Backup data, you will need to enable the appropriate processing option either when you add the evidence or later by using Additional Analysis.

Note: You will need the user's password in order to open any encrypted backup files. We currently do not decrypt iOS Backup files.

Expanding iOS Backup Data

To Expand iOS Backup Data:

1. During processing, or in *Additional Analysis*, open the *Evidence Processing* window.
2. Check the **Expand Compound Files** option.
3. Click on the **Expansion Options** box and check the box for **iOS Backup**.
4. Click **Ok** and process the evidence.

Locating iOS Backup Data

To Locate iOS Backup Data:

1. In the *Explore Tab*, open the evidence and navigate to the **Manifest.db** file.
2. Select any folder to view iOS Backup evidence.

Important: When looking at iOS Backup files in the Overview Tab, these files will not be classified as Mobile Phone files. They will be classified as the standard file category for each type of file found on the phone.

Working with Facebook Messenger (Android)

To expand Facebook Messenger App data on an Android phone, you will need to enable the appropriate processing option either when you add the evidence or later by using Additional Analysis.

Expanding Facebook Messenger (Android) Data

To Expand Facebook Messenger (Android) Data:

1. During processing, or in *Additional Analysis*, open the *Evidence Processing* window.
2. Check the **Expand Compound Files** option.
3. Click on the **Expansion Options** box and check the box for **Facebook Messenger (Android)**.
4. Click **Ok** and process the evidence.

Note: There is a known issue within Facebook that deletes the last names of contacts and substitutes the first name for the last name. This is a bug within Facebook, but the behavior will persist when exploring evidence within the Examiner.

Locating Facebook Messenger (Android) Data

To Locate Facebook Messenger (Android) Data:

1. In the *Explore Tab*, open the phone evidence and navigate to the following path:

   [root] > data > com.facebook.orca > databases > threads_db2
2. Open the **threads_db2** folder. Select either the **Contacts, inbox**, or **pending** folder to view the data.

Important: The *pending* folder will not always have data in it.

To View Facebook Messenger (Android) Contacts:

1. Navigate to and highlight the **Contacts** folder, as described above.
2. The *File List* will show the available contacts. Select a contact, and the associated information for that contact will appear in the *File Content* pane.

Note: The Profile URLs shown for Facebook Messenger (Android) contacts are external and unusable because they require Facebook cookies to work.

To View Facebook Messenger (Android) Conversations:

1. Navigate to the **inbox** folder, as described above.
2. Select a conversation. It will populate as individual messages in the *File List*. The entire conversation will appear in Cool HTML in the *File Content* pane.

Note: The Attachments Column will contain links, not actual items. These links are external (stored in the cloud) and will need the Facebook cookies to work, meaning you must be logged in under the proper Facebook account to view them. The Pending Send Media Attachment Column will also have a link to the image. But since this image was pending, it might be available somewhere in the evidence.

Viewing Data in Volume Shadow Copies

You can examine data that is contained in NTFS Volume Shadow Copies.

See Examining Data in Volume Shadow Copies on page 147.

Viewing Microsoft Office and Adobe Metadata

You can examine metadata from Microsoft Office and Adobe documents. This data is processed by default, but you must use the following method to view it.

To view Microsoft Office and Adobe Metadata

1. In the examiner, open one of the following:
   - The **Overview** tab > **File Category** > **Documents** > **Adobe Documents**
   - The **Overview** tab > **File Category** > **Documents** > **Microsoft Documents**
2. In the *File List*, click the *Check all files in the current list* icon.
3. Click on the *Column Settings* icon.
   See Managing Columns on page 480.
4. Either create a new column template or edit an existing one.
5. In the **Available Columns** list, expand **Office-specific Features** or **All Features**.
6. Add the desired columns to the template.
   For example, to add columns for Adobe metadata, use the following:
   - All Features
     - Meta-data - Date Created
     - Meta-data - Date Modified
7. Click **OK**.
8. Select the template name you just configured and click **Apply**.
   This applies the template to the *File List*.
9. Click **Close**.
10. You will now see the meta-data information in the columns for each record.

When viewing the expanded files, you can use the following columns in the File List to display detailed data

Microsoft Office and Adobe Metadata Columns

Microsoft Office documents	• CreateTime (Content created) • EmbeddedComments (PPT files) • HiddenColumnsRows (Excel files) • HiddenWorkSheets (Excel files) • LastPrinted • LastSavedTime (Date last saved) • RevisionNumber • TotalEditingTime (Word and PPT) • TrackChanges • From file Origin properties

Microsoft Office and Adobe Metadata Columns	
Adobe files	• Meta-data - DateCreated • Meta-data - DateModified

About Windows 8 and 10 Keyword Searches

Windows 8 and Windows 10 have added the ability to perform an advanced search query. These advanced search query files are now parsed automatically during forensic processing.

Advanced Query Searches are saved by Windows in the **Admin > Searches** folder. There are two default searches found in Windows 10. These are the Indexed Locations and Everywhere files.

Chapter 25

Bookmarking Evidence

This chapter includes the following topics

- About Bookmarks (page 364)
- About Timeline Bookmarks (page 364)
- Using the Bookmarks Tab (page 371)
- Creating a Bookmark (page 365)
- Viewing Bookmark Information (page 371)
- Bookmarking Selected Text (page 372)
- Adding to an Existing Bookmark (page 373)
- Creating Email or Email Attachment Bookmarks (page 374)
- Adding Email and Email Attachments to Existing Bookmarks (page 374)
- Moving a Bookmark (page 375)
- Copying a Bookmark (page 375)
- Deleting a Bookmark (page 375)
- Deleting Files from a Bookmark (page 375)

About Bookmarks

A bookmark is a group of files that you want to reference in your case. These are user-created and the list is stored for later reference, and for use in the report output. You can create as many bookmarks as needed in a case. Bookmarks can be nested within other bookmarks for convenience and categorization purposes.

Bookmarks help organize the case evidence by grouping related or similar files. For example, you can create a bookmark of graphics that contain similar or related graphic images. The *Bookmarks* tab lists all bookmarks that have been created in the current case.

Bookmarks only apply to the case they are created in.

About Timeline Bookmarks

When creating bookmarks, you can also create a Timeline type of bookmark. A Timeline bookmark lets you show the chronological relationships of the files in your case. When you create a Timeline bookmark, you can record the Create Date, Accessed Date, and Modified Date for files as individual items. You can then export that data to a CSV report file. Each action (create, accessed, modified) for each file is a separate item in the report.

When sorted by the date and time, the CSV report file presents a chronological timeline of the actions of the evidence files in your case.

For example, you can create a bookmark of files that were downloaded from the internet. The report shows when the files were downloaded (created) and the time interval between then and when they were last accessed. You can also see if and when the files were modified.

You can also add manual timeline data. Manual timeline data lets you add items to your timeline that may not be represented by the files in your case. For example, you may have phone logs that show when relevant phone calls were placed. You can add those phone calls as manual timeline items so that they appear in your report along with the file information in the case.

You can use the exported CSV file produce you own chronological timeline of the evidence in the case. This can present a clearer view of how certain events happened which can help investigators communicate to the jurors and judge on their case.

The CSV report file includes the following data as columns:

- The date/time stamp of the file action
- The type of file action (Modified, Accessed, Created, or Other)
  The Other category is used for manual timeline entries.
- The bookmark name
- The filename
- Any comments that you manually entered for each item

A bookmark can either be a timeline bookmark or a regular bookmark, but not both.

Creating a Bookmark

To create a bookmark

1. In the *File List* view , select the files that you want to add to the bookmark.
   You can either highlight the files that you want to include, check the boxes of the files that you want to include, or do nothing to include all files.
2. Right-click on a selected file in the *File List* view and click *Create Bookmark*.
3. Enter the information about the bookmark.
   See Bookmarks Dialog Options on page 367.
4. Click **OK**.

> **Note:** Applying filters to a group of listed files for bookmarking can speed the process. The *All Highlighted* setting does not work in this instance. Enabling this feature would significantly slow the response of the program. Instead, use either the *Checked Files* filter, or the *All Files Listed* filter.

About Empty Bookmarks

You can create bookmarks that contain only the name and location of the bookmark. These are called Empty Bookmarks. Empty Bookmarks allow you to add “placeholders” while investigating a case. This feature makes it easy to mark your place and come back to it later. For example, while investigating a fraud case, you notice an email that may or may not be pertinent to your investigation. Creating an Empty Bookmark allows you to quickly “save your place” and come back later when you have more time to delve into that evidence.

You can also use Empty Bookmarks to format your Bookmarks tree. This allows you to better organize your bookmarks. For example, you may be investigating documents, video, graphics, and emails. You could create an Empty Bookmark called Documents, under which you would place all of your document-related bookmarks. Then, you would create an Empty Bookmark called Video, under which you would place all of your video-related bookmarks. Continue creating Empty Bookmarks until you have a manageable Bookmark tree.

There are two ways to create Empty Bookmarks, creating the Empty Bookmark from the Bookmarks tab or in the *Create New Bookmark* dialog.

To create an Empty Bookmark from the Bookmarks tab

1. In *Evidence Explorer*, click the *Bookmarks* tab.
2. Right-click the bookmark under which to create the Empty Bookmark.
3. Click **Create Empty Bookmark**.
4. Enter a name for the Empty Bookmark and click **OK**.
   You add and save additional bookmark information to an Empty Bookmark at anytime by using the Bookmark Information pane.

To create an Empty Bookmark in the Create New Bookmark dialog

1. Create a bookmark. See Creating a Bookmark on page 365.
2. In Files to Include, select **None**.
3. Save the bookmark.

Bookmarks Dialog Options

Options of the Bookmark Information Pane

Field	Description
Bookmark Name	The name of the bookmark.
Bookmark Comment	Comments about the bookmark or its contents. Bookmark Comments are created in an HTML editor. HTML allows you to format your comments within the bookmark and for any subsequent reports. See Bookmark Comments HTML Editor on page 369.
Files to Include	Specify which files in the File List to include in this bookmark. You can select one of the following: ● All Highlighted - Includes only the highlighted items. ● All Checked - Includes only the checked items. ● All Listed - Includes all items in the File List. ● None - Creates an Empty Bookmark.
Timeline Bookmark	Select this option to make this a Timeline bookmark. If you select the Timeline tab, this options is selected automatically. A bookmark can either be a Timeline Bookmark or a regular bookmark, but not both.
Select Existing Bookmark	Select the parent bookmark under which you would like to save the bookmark. A default shared tree for bookmarks available to all investigators is created, and a bookmark tree specific to the case owner is created. If the bookmark is related to an older bookmark it can be added under the older bookmark, with the older bookmark being the parent, or it can be saved as a peer.
Comments tab	This lets you configure elements of a standard bookmark.
File Comments	You can assign a comment to each file in the bookmark. Comments are created in an HTML editor. HTML allows you to format your comments within the bookmark and for any subsequent reports. See Bookmark Comments HTML Editor on page 369.
Supplementary Files	You can add external, supplementary files associated with the bookmark. Options are: ● *Attach*: Allows the investigator to add external supplementary files to the bookmark. The attached files appear in the Supplementary Files pane and are copied to the case folder. ● *Remove:* Removes a selected supplementary file from the bookmark.

Options of the Bookmark Information Pane (Continued)

Field		Description
	Also include	If applicable, you can include the following: • Parent index.dat The option to include Parent index.dat is only available if you have selected to bookmark an index entry, for example a cookie. This option includes the entry's parent index.DAT file in the bookmark. • Email Attachments - If one of the items selected is an email with attachments, this will include all of the attachments that the email has. • Parent Email - If one of the items selected is an email attachment object, selecting this option will include the parent email. • Exclude Selected OCR Extractions The Exclude Selected OCR Extractions check box appears only when OCR- extracted files have been selected when creating a new or adding to an existing bookmark. If, instead, you have selected graphic files, and have not selected their OCR counterparts, the check box for OCR Extractions of selected Graphics will be active and available. • Actual Source File This option lets you include the parent child of a processing-generated file. See Relating Generated Files to Original Files on page 333.
	Bookmark Selection in File	Check this item to have the highlighted text in a file automatically highlighted when the bookmark is re-opened. The highlighted text also prints in the report. The selected text that will be included displays in the text box below the check box.
Timeline tab		This lets you configure elements of a Timeline bookmark.
	Create Date	Select this option to record the date and time that the file was created.
	Accessed Date	Select this option to record the date and time that the file was last accessed.
	Modified Date	Select this option to record the date and time that the file was last modified.
	Object Timeline Comments	You can assign a comment to each file timestamp in the bookmark. Comments are created in an HTML editor. HTML allows you to format your comments within the bookmark and for any subsequent reports. See Bookmark Comments HTML Editor on page 369. The timeline comments are shown in the timeline report anchored to each date, and each date being used will crate a new row in the text report.
	Manual Timeline Data	In this section, you can add manual timeline entries that are not available as items in the *File List*. For example, you may have access to phone records and you can add call histories as individual manual entries. You enter the date and time of the items and then in the CSV, they are displayed chronologically with the other items in your bookmark. **Note:** Manual items are listed as *Other* in the report.

Options of the Bookmark Information Pane (Continued)

Field		Description
	Manual Timeline Comments	(Optional) Enter a comment or description to enter a Manual Timeline item. Comments are created in an HTML editor. HTML allows you to format your comments within the bookmark and for any subsequent reports. See Bookmark Comments HTML Editor on page 369.
	Manual Date	Enter the date of the Manual Timeline item. You can click the arrow to open a calendar.
	Manual Time	Enter the time of the Manual Timeline item.
	Add	Click **Add** to save the Manual Timeline item. The item is added to the Manual Timeline Entries list.
	Remove	Highlight a Manual Timeline entry and click **Delete** to remove it from the list.
	Manual Timeline Entries	The list Manual Timeline items that you have added.
Select Bookmark Parent		Select the parent bookmark under which you would like to save the bookmark. There are two default bookmark parents: ● A *Shared* tree that is available to all investigators ● A bookmark tree specific to the logged-in-user Administrators and Case Administrators can see and use all bookmarks in a case. If the bookmark is related to an older bookmark it can be added under the older bookmark, with the older bookmark being the parent, or it can be saved as a peer.

Bookmark Comments HTML Editor

The HTML Editor for Bookmark Comments allows you to format Bookmark Comments using HTML.

Important: You are required to use the HTML Editor when entering Bookmark Comments, with or without formatting.

To enter Bookmark Comments

1. In *Evidence Explorer*, click the **Bookmarks** tab.
2. Highlight (click) a bookmark from the *Bookmarks* pane.
3. Click the **Edit** button next to the Comment field.
   The HTML Editor appears.
4. Enter and/or format your comments using formatting options. You can also format your comments directly in HTML by clicking **Source**. For a brief description of each HTML formatting option, click **Help** in the HTML Editor.
5. Click **Done** in the HTML Editor when finished.

Note: ALWAYS click **Done** in the HTML Editor to exit the editor and keep your comments. You still need to save the Bookmark (**Save Changes**) to keep the comment in the Bookmark.

Viewing Bookmark Information

The *Bookmark Information* pane displays information about the selected bookmark and the selected bookmark file. The data in this pane is editable by anyone with sufficient rights.

Select a bookmark in the *Bookmarks* tree view of the *Bookmarks* tab, or in the *Bookmarks* node in the tree of the *Overview* tab to view information about a bookmark. The *Overview* tab view provides limited information about the bookmarks in the case. The *Bookmark* tab provides all information about all bookmarks in the case. In the *Bookmark* tab, the *Bookmark Information* pane displays the Bookmark Name, Creator Name, Bookmark Comment, and Supplementary files. When selected, a list of files contained in the bookmark displays in the File List. If you select a file from the File List, the comment and selection information pertaining to that file displays in the *Bookmark Information* pane.

Bookmarked files display in a different color in the *File List* pane than non-bookmarked files for easy identification.

Change any of the information displayed from this pane. Changes are automatically saved when you change the bookmark selection.

In the File List, bookmarked items display in a different color for easy identification. You may need to refresh the view to force a rewrite of the screen for the different color to display. Forcing a rewrite would impact the overall performance of the program.

Creating a Timeline Bookmark Report

After you have created Timeline Bookmarks, you can crate Timeline Bookmark Reports. The reports are in CSV format. You can specify one or more Timeline Bookmarks for each report. You specify one or more Timeline Bookmarks for each report. You specify the location and name of the saved CSV report.

See About Timeline Bookmarks on page 364.

To create a timeline Bookmark Report

1. In the Examiner, click **File** > **Timeline** > **Report**.
2. Select one or more Timeline Bookmarks to use for the report.
3. (Optional) Select one of the following
   - *Select All Children* - This selects all of the children of the selected bookmarks in the bookmark tree.
   - *Clear All Children* - This clears all of the children of the selected bookmarks in the bookmark tree.
4. Click **Select** to select an output folder.
   4a. Select the folder to save the report in.
   4b. Specify the name of the report or use the default Timeline Report name.
5. Click **Generate** to save the report.

Using the Bookmarks Tab

You can use the Bookmark tab to view, create, and edit bookmarks.

Bookmarking Selected Text

Bookmarked selections are independent of the view in which they were made. Select hex data in the Hex view of a bookmarked file and save it; bookmark different text in the Filtered view of the same file and save that selection as well.

To add selected text in a bookmark

1. Open the file containing the text you want to select.
2. From the Natural, Text, Filtered or Hex views, make your selection.

   Note: If the file is a graphic file, you will not see, nor be able to make selections in the Text or the Natural views.

3. Click **Create Bookmark** in the File List toolbar to open the *Create New Bookmark* dialog.
4. When creating your bookmark, check **Bookmark Selection in File.**
5. To save selected content, choose the view that shows what you want to save, then highlight the content to save.
6. Right-click the selected content. Click **Save As**.
7. In the *Save As* dialog, provide a name for the selection and click **Save**.
   The selection remains in the bookmark.

Bookmarking Video Thumbnails

You can bookmark Video Thumbnails by creating a new bookmark or adding to an existing bookmark. By default, Video Thumbnails that are added to Bookmarks play from the location thumbnail to end of the video. You can update, change the start/end times, or remove the thumbnail from within the bookmark. You can also export your video thumbnails to your report.

See Using the Video Thumbnails Pane on page 330.

See About Bookmarks on page 364.

See Adding Bookmarks to a Report on page 489.

Adding a Video Thumbnail to a New or Existing Bookmark

To add a Video Thumbnail to a new or existing Bookmark

1. From the *Evidence Explorer*, click the *Video* tab.
2. Right-click the video thumbnail for the Bookmark.
3. Click either:
   - **Create Bookmark**. See Creating a Bookmark on page 365.
   - **Add to Bookmark**. See Adding to an Existing Bookmark on page 373.
4. Follow the instructions for creating and/or adding to a Bookmark.

About Updating/Removing Bookmarked Video Thumbnails

Once there are Video Thumbnails in a Bookmark, you can update (change) the Video Thumbnail or remove it.

Note: You cannot add a selection of a video from the Bookmark's Natural Viewer using the **Add Selection** button. To add a video thumbnail to a bookmark, see Adding a Video Thumbnail to a New or Existing Bookmark (page 372).

To update a Video Thumbnail in a Bookmark

1. From the *Evidence Explorer*, click the *Bookmarks* tab.
2. In the *Bookmarks* pane, navigate to and highlight the Bookmark containing the Video Thumbnail(s).
3. In the *File List* pane, highlight the video from which the thumbnails were created.
4. In the *Bookmark Information* > *Selections* pane, click (highlight) the thumbnail (selection).
5. In the *File Content* > *Natural Viewer*, click Play ( ) and then Pause.
6. Click **Update Section**.
7. Enter a Start and/or End Time.
8. Click **OK**.

To remove a Video Thumbnail from a Bookmark

1. From the *Evidence Explorer*, click the *Bookmarks* tab.
2. In the *Bookmarks* pane, navigate to and highlight the Bookmark containing the Video Thumbnail(s).
3. In the *File List* pane, click (highlight) the video from which the thumbnails were created.
4. In the *Bookmark Information* > *Selections* pane, click (highlight) the thumbnail (selection).
5. Click **Remove Selection**.
6. Confirm the change.

Adding to an Existing Bookmark

Sometimes additional information or files are desired in a bookmark.

To add to an existing bookmark

1. Select the files to be added to the existing bookmark.
2. Right-click the new files.
3. Click **Add to Bookmark**.
4. When available (depending on the type of files you are adding), make selections for **Files to Add**, **Also Include**, **OCR Extractions of Selected Graphics,** and **Bookmark Selection in File**.
5. Open the parent bookmark tree.
6. Select the child bookmark to add the file or information to.
7. Click **OK**.

Creating Email or Email Attachment Bookmarks

When bookmarking an email, you can also add and bookmark any attachments. You can also include a parent email when you bookmark an email attachment.

To create a bookmark for an email, follow the steps for creating a bookmark. Select the email to include in the bookmark. Right-click and choose **Create Bookmark**. Note that by default, the **Email Attachments box** is active, but unmarked. If only the parent email is needed, the **Email Attachments** box should remain unselected.

Complete the bookmark creation normally by naming the bookmark, selecting the bookmark parent, then clicking **OK**.

If you need to bookmark only an attachment of the email, select and right-click on the attachment. Choose **Create Bookmark**. For more information on creating bookmarks, see, Creating a Bookmark (page 365).

Notice that the Parent Email box is automatically active, allowing you to include the parent email if it is not part of the selection you have already made. If the Parent Email box is checked, and there is more than one attachment, the Email Attachments box becomes active as well, allowing you to also include **all** attachments to the parent email. To add only the originally selected attachment to the bookmark, do not check the Parent Email box.

Adding Email and Email Attachments to Existing Bookmarks

To add an email to a bookmark, select the email to add, then right-click on the email and choose **Add To Bookmark**. Note that if emails are selected, but their attachments are not selected, the **Email Attachments** box is active, but not marked. If only the parent email is needed, the **Email Attachments** box can remain unselected. If you have selected only the attachment, include the attachment's parent email by marking the **Parent Email** box.

One way to be sure to find the exact items you want is to highlight an interesting item in the File List view in one tab, then right-click on it and select **View This Item in a Different List**. Click on **Email** and you are taken to the Email tab with the selected email highlighted in the File List view, and displayed in the Natural tab in the File Content pane. In the Email Attachments pane on the right that file is displayed, along with its role; whether it is a parent email, part of the email thread, or an attachment.

If only an attachment of an email is needed to be added to the bookmark, select the attachment and follow the instructions for adding to a bookmark.

Moving a Bookmark

To move a bookmark

1. From either the *Bookmark* tab or the Overview tab, select the bookmark you want to move.
2. Drag the bookmark to the desired location and then release the mouse button.

Copying a Bookmark

To copy a bookmark

1. From either the *Bookmark* tab or the *Overview* tab, select the bookmark you want to copy.
2. Using the right mouse button, drag the bookmark to the desired location and release the mouse button.

Deleting a Bookmark

To delete a bookmark

1. In the *Bookmark* tab, expand the bookmark list and highlight the bookmark to be removed.
2. Do one of the following:
   - Press the **Delete** key.
   - Right-click on the bookmark to delete, and click **Delete Bookmark**.

Deleting Files from a Bookmark

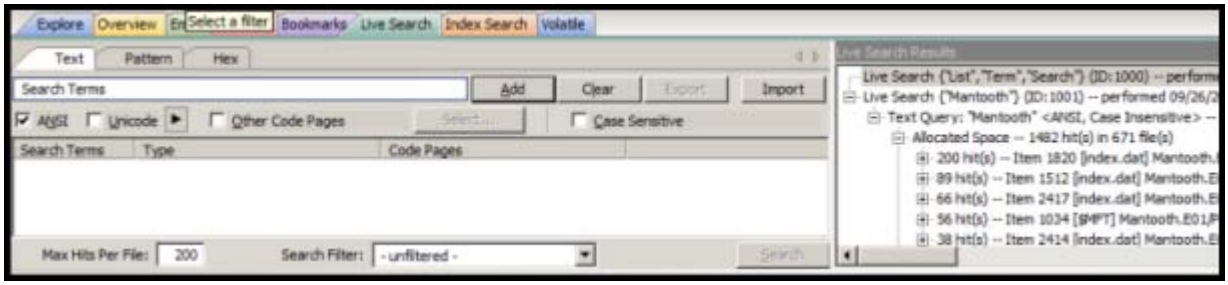
To delete files from a bookmark

1. From either the *Overview* tab or the *Bookmarks* tab, open the bookmark containing the file you want to delete.
2. Right-click the file in the *Bookmark File List* pane.
3. Do one of the following:
   - Select **Remove from Bookmark**.
   - Press the Delete key on your keyboard. You will be prompted, “Are you sure you want to delete files from this bookmark?” Click **Yes**.
   - Deleting a file from a bookmark does not delete the file from the case.

Chapter 26

Searching Evidence with Live Search

Searching evidence for information pertaining to a case can be one of the most crucial steps in the examination. An index search gives rapid results, and a live search includes options such as text searching and hexadecimal searching. You can view search results from the *File List* and *File Contents* views of the *Search* tab.



The Live Search is a process involving a bit-by-bit comparison of the entire evidence set with the search term.

This chapter includes the following topics

- Conducting a Live Search (page 376)
- Live Text Search (page 377)
- Live Hex Search (page 379)
- Live Pattern Search (page 380)
- Using Pattern Searches (page 380)
- Predefined Regular Expressions (page 383)
- Creating Custom Regular Expressions (page 385)

Conducting a Live Search

The live search takes slightly more time than an index search because it involves a bit-by-bit comparison of the search term to the evidence. A live search is flexible because it can find patterns of non-alphanumeric characters, including those that are not generally indexed. It is powerful because you can define those patterns to meet your needs in an investigation.

Note: If a case was originally processed using distributed processing, when a reviewer conducts a live search, the system will first attempt to use the computer with the distributed processing engine, but if it is not available, it will use the reviewer's local computer to conduct the search.

Live Text Search

A *Text* search finds all strings that match an exact entry, such as a specific phone number (801-377-5410). When conducting a Live Text Search, there are no arrows to click for operand selection.

A Live Text Search gives you options such as ANSI, Unicode with UTF-16 Little Endian, UTF-16 Big Endian, and UTF-8. The latter two are always case-sensitive. You can also choose from a list of other Code Pages to apply to the current search. In addition, you can select Case Sensitivity for any Live Text Search.

Note: When entering Chinese characters into search, you must have both ANSI and Unicode options selected.

The difference between a Pattern search and a Text search is that a text search searches for the exact typed text, there are no operands so the results return exactly as typed. For example, a **simple** *Pattern* search allows you to find all strings that match a certain pattern, such as for any 10-digit phone number **(nnn-nnn-nnnn**), or a nine-digit social security number (**nnn-nn-nnnn**).

More **complex** *Pattern* searches (“regex”) require specific syntax. See Live Pattern Search (page 380).

Search terms can be entered then exported as XML files, then imported at any time, or with any case. Text files can be imported and used in Live Search, however the Live Search Export feature supports only XML format.

Note: When importing TXT files that the search of those terms depend on the specific tab your in. (ie If I have a few hex terms and import the TXT list into Live Search in the Patterns tab), the search is run as a pattern search and not hex.

To Conduct a Live Text search

1. In the Live Search tab, click the **Text** tab.
   In the Text or Pattern tabs, you can check the character sets to include in the search.
2. If you want to include sets other than ANSI and Unicode, check **Other Code Pages** and click **Select.**
3. Select the needed sets.
4. Click to include **EBCDIC, Mac**, and **Multibyte** as needed.
5. Click **OK** to close the dialog.
6. Check **Case Sensitive** if you want to search specifically uppercase or lowercase letters as entered. Case is ignored if this box is not checked.
7. Enter the term in the *Search Term* field.
8. Click **Add** to add the term to the *Search Terms* window.
9. Click **Clear** to remove all terms from the *Search Terms* window.
10. Repeat Steps 7, 8, and 9 as needed until you have your search list complete.
    When you have added the search terms for this search, it is a good idea to export the search terms to a file that can be imported later, saving the time of re-entering every item, and the risk of errors. This is particularly helpful for customized pattern searches.
11. In the Max Hits Per File field, enter the maximum number of search hits you want listed per file. The default is 200. The range is 1 to 65,535. If you want to apply a filter, do so from the Filter drop-down list in the bar below the Search Terms list. Applying a filter speeds up searching by eliminating items that do not match the filter. The tab filter menu has no effect on filtering for searches.
12. Click **Search**.
13. Select the results to view from the Live Search Results pane. Click the plus icon (+) next to a search line to expand the branch. Individual search results are listed in the Live Search Results pane, and the

corresponding files are listed in the File List. To view a specific item, select the hit in the search results. Selected hits are highlighted in the Hex View tab.

14. When a search is running you can click **View > Progress Window** to see how the job is progressing.

> **Note:** In the progress window, you can **Pause**, **Resume**, and **Cancel** jobs, in addition to closing the window. (**Pause** and **Resume** are the same button, but the label changes depending on processing activity.)

> **Note:** Mark the **Remove when finished** check box to take completed jobs off the list for housekeeping purposes.

15. When processing is complete, return to the Live Search tab to review the results.

    Right-click on a search result in the Live Search Results pane to display more options. The available right-click options are as follows:

Option	Description
Create Bookmark	Opens the *Create New Bookmark* dialog.
Copy to Clipboard	Opens a new context-sensitive menu. Options are:
	• All Hits In Case • All Hits In Search • All Hits In Term • All Hits In File • All File Stats In Case • All File Stats In Search • All File Stats In Term
Export to File	Opens a new context-sensitive menu. Options are:
	• All Hits In Case • All Hits In Search • All Hits In Term • All Hits In File • All File Stats In Case • All File Stats In Search • All File Stats In Term
Set Context Data Width	Opens the *Data Export Options* window. Allows you to set a context width from 32 to 2000 characters within which it can find and display the search hit.
Export Search Term	Select to export a search term list that can be imported into this or other cases.
Delete All Search Results	Deletes all search results from the Live Search Results pane.
Delete this Line	Deletes only the highlighted search results line from the Live Search Results pane.

Searching before the case has finished processing will return incomplete results. Wait to search until the case has finished processing and the entire body of data is available.

> **Note:** Search terms for pre-processing options support only ASCII characters.

Live Hex Search

Hexadecimal (Hex) format includes pairs of characters in a base 16 numeric scheme, 0-9 and a-f. Hex searching allows you to search for repeating instances of data in Hex-format, and to save Hex-format data search strings to an XML file and re-use it in this or other cases.

Click the **Hex** (Hexadecimal) tab to enter a term by typing it directly into the search field, by clicking the Hexadecimal character buttons provided, or by copying hex content from the hex viewer of another file and pasting it into the search box. Click **Add** to add the hex string to the search terms list.

The instructions for conducting a live search on the hex tab are similar to conducting searches on the Pattern tab. Remember, when searching for hexadecimal values, a single alphabetic or numeric text character is represented by hex characters in pairs.

To do a Hex search

1. In the *Live Search* tab, click the **Hex** tab.
2. Add Hex search strings using the keyboard or using the Alpha-numeric bar above the *Search Terms* box.
3. Click **Add** to add the term to the *Search Terms* window.
4. Click **Clear** to remove all terms from the *Search Terms* window.
5. Repeat Steps 2, 3, and 4 as needed until you have your search list complete.
6. When you have added the search terms for this search, it is a good idea to export the search terms to a file that can be imported later, saving the time of re-entering every item, and reduces the risk of errors. This is particularly helpful for customized pattern searches.
7. In the Max Hits Per File field, enter the maximum number of search hits you want listed per file. The default is 200. The range is 1 to 65,535. If you want to apply a filter, do so from the Filter drop-down list in the bar below the Search Terms list. Applying a filter speeds up searching by eliminating items that do not match the filter. The tab filter menu has no effect on filtering for searches.
8. Click **Search**.
9. Select the results to view from the Live Search Results pane. Click the plus icon (+) next to a search line to expand the branch. Individual search results are listed in the Live Search Results pane, and the corresponding files are listed in the File List. To view a specific item, select the file in the search results. All search results are highlighted in the Hex View tab.

Live Pattern Search

The more complex Live Pattern “Regex” style search can be used to create pattern searches, allowing forensics analysts to search through large quantities of text information for repeating strings of data such as:

- Telephone Numbers
- Social Security Numbers
- Computer IP Addresses
- Credit Card Numbers

In the Live Search tab, click the **Pattern** tab. Each has different options.

The patterns consist of precise character strings formatted as mathematical-style statements that describe a data pattern such as a credit card or social security number. Pattern searches allow the discovery of data items that conform to the pattern described by the expression, rather than what a known and explicitly entered string looks for.

These pattern searches are similar to arithmetic expressions that have operands, operators, sub-expressions, and a value. For example, the following table identifies the mathematical components in the arithmetic expression, 5/((1+2)*3).

Regex Pattern Search Components

Component	Example
Operands	5, 1, 2, 3
Operators	/, ( ), +, *
Sub-Expressions	(1+2), ((1+2)*3)
Value	Approximately 0.556

Like the arithmetic expression in this example, pattern searches have operands, operators, sub-expressions, and a value.

Note: Unlike arithmetic expressions, which can only have numeric operands, operands in pattern searches can be any characters that can be typed on a keyboard, such as alphabetic, numeric, and symbol characters.

Using Pattern Searches

A pattern search can consists of operands. The search engine searches left to right.

Operators let regular expressions search patterns of data rather than for specific values. For example, the operators in the following expression enable the search engine to find all Visa and MasterCard credit card numbers in case evidence files:

```
\<((\d\d\d\d)[\– ]){3}\d\d\d\d\>
```

Without the use of operators, the search engine could look for only one credit card number at a time.

Visa and MasterCard Regular Expressions

Operands	\–, spacebar space
Operators	\, \<, <, ( ), [ ], {3}, \>
Sub-expressions	(\d\d\d\d), ((\d\d\d\d)[\–])
Value	Any sequence of sixteen decimal digits that is delimited by three hyphens and bound on both sides by non-word characters (**xxxx–xxxx–xxxx–xxxx**).

As the pattern search engine evaluates an expression in left-to-right order, the first operand it encounters is the backslash less-than combination (\<). This combination is also known as the begin-a-word operator. This operator tells the search engine that the first character in any search hit immediately follows a non-word character such as white space or other word delimiter.

Note: A precise definition of non-word characters and constituent-word characters in regular expressions is difficult to find. Consequently, experimentation may be the best way to determine if the forward slash less-than (**\<**) and forward slash greater-than (**\>**) operators help find the data patterns relevant to a specific searching task. The hyphen and the period are examples of valid delimiters or non-word characters.

The begin-a-word operator illustrates one of two uses of the backslash or escape character (\ ), used for the modification of operands and operators. On its own, the left angle bracket (<) would be evaluated as an operand, requiring the search engine to look next for a left angle bracket character. However, when the escape character immediately precedes the (<), the two characters are interpreted together as the begin-a-word operator by the search engine. When an escape character precedes a hyphen (-) character, which is normally considered to be an operator, the two characters (\-) require the search engine to look next for a hyphen character and not apply the hyphen operator (the meaning of the hyphen operator is discussed below).

The parentheses operator ( ) groups together a sub-expression, that is, a sequence of characters that must be treated as a group and not as individual operands.

The **\d** operator, which is another instance of an operand being modified by the escape character, is interpreted by the search engine to mean that the next character in search hits found may be any decimal digit character from 0-9.

The square brackets ([ ]) indicate that the next character in the sequence must be one of the characters listed between the brackets or escaped characters. In the case of the credit card expression, the backslash-hyphen-spacebar space ([\-*spacebar space*]) means that the four decimal digits must be followed by either a hyphen or a spacebar space.

The {3} means that the preceding sub-expression must repeat three times, back to back. The number in the curly brackets ({ }) can be any positive number.

Finally, the backslash greater-than combination (\>), also known as the end-a-word operator, means that the preceding expression must be followed by a non-word character.

Sometimes there are ways to search for the same data using different expressions. It should be noted that there is no one-to-one correspondence between the expression and the pattern it is supposed to find. Thus the preceding credit card pattern search is not the only way to search for Visa or MasterCard credit card numbers.

Because some pattern search operators have related meanings, there is more than one way to compose a pattern search to find a specific pattern of text. For instance, the following pattern search has the same meaning as the preceding credit card expression:

```
\<((\d\d\d\d)(\–| )){3}\d\d\d\d\>
```

The difference here is the use of the pipe (|) or union operator. The union operator means that the next character to match is either the left operand (the hyphen) or the right operand (the spacebar space). The similar meaning of the pipe (|) and square bracket ([ ]) operators give both expressions equivalent functions.

In addition to the previous two examples, the credit card pattern search could be composed as follows:

```
\<\d\d\d\d(\–| )\d\d\d\d(\–| )\d\d\d\d(\–| )\d\d\d\d\>
```

This expression explicitly states each element of the data pattern, whereas the {3} operator in the first two examples provides a type of mathematical shorthand for more succinct regular expressions.

Predefined Regular Expressions

Many predefined regular expressions are provided for pattern searching.

Examples of Predefined Regular Expressions	
• U.S. Social Security Numbers	• IP Addresses
• U.S. Phone Numbers	• Visa and MasterCard Numbers
• U.K. Phone Numbers	• Computer Hardware MAC Addresses

Social Security Number

The pattern search for Social Security numbers follows a relatively simple model:

```
\<\d\d\d[\– ]\d\d[\– ]\d\d\d\d\>
```

This expression reads as follows: find a sequence of text that begins with three decimal digits, followed by a hyphen or spacebar space. This sequence is followed by two more decimal digits and a hyphen or spacebar space, followed by four more decimal digits. This entire sequence must be bounded on both ends by non-word characters.

U.S. Phone Number

The pattern search for U.S. phone numbers is more complex:

```
((\<1[\–\. ])?(\(|\<)\d\d\d[\)\.\–/ ] ?)?\<\d\d\d[\.\– ]\d\d\d\d\>
```

The first part of the above expression,

```
((\<1[\–\. ])?(\(|\<)\d\d\d[\)\.\–/ ] ?)?,
```

means that an area code may or may not precede the seven digit phone number. This meaning is achieved through the use of the question mark (?) operator. This operator requires that the sub-expression immediately to its left appear exactly zero or one times in any search hits. This U.S. Phone Number expression finds telephone numbers with or without area codes.

This expression also indicates that if an area code is present, a number one (1) may or may not precede the area code. This meaning is achieved through the sub-expression (\<1[\–\.])?, which says that if there is a “1” before the area code, it will follow a non-word character and be separated from the area code by a delimiter (period, hyphen, or spacebar space).

The next sub-expression, (\(|\<)\d\d\d[\)\.\–/] ?, specifies how the area code must appear in any search hits. The \(|\<) requires that the area code begin with a left parenthesis or other delimiter. The left parenthesis is, of necessity, escaped. The initial delimiter is followed by three decimal digits, then another delimiter, a right parenthesis, a period, a hyphen, a forward slash, or a spacebar space. Lastly, the question mark (?) means that there may or may not be one spacebar space after the final delimiter.

The latter portion of this expression, \<\d\d\d[\.\–]\d\d\d\d\>, requests a seven-digit phone number with a delimiter (period, hyphen, or spacebar space) between the third and fourth decimal digit characters. Note that typically, the period is an operator. It means that the next character in the pattern can be any valid character. To specify an actual period (.), the character must be escaped (\ .). The backslash period combination is included in the expression to catch phone numbers delimited by a period character.

IP Address

An IP address is a 32-bit value that uniquely identifies a computer on a TCP/IP network, including the Internet. Currently, all IP addresses are represented by a numeric sequence of four fields separated by the period character. Each field can contain any number from 0 to 255. The following pattern search locates IP addresses:

```
\<[1-2]?[0-9]?[0-9]\.[1-2]?[0-9]?[0-9]\.[1-2]?[0-9]?[0-9]\.[1-2]?[0-9]?[0-9]\>
```

The IP Address expression requires the search engine to find a sequence of data with four fields separated by periods (.). The data sequence must also be bound on both sides by non-word characters.

Note that the square brackets ([ ]) still behave as a set operator, meaning that the next character in the sequence can be any one of the values specified in the square brackets ([ ]). Also note that the hyphen (-) is not escaped; it is an operator that expresses ranges of characters.

Each field in an IP address can contain up to three characters. Reading the expression left to right, the first character, if present, must be a 1 or a 2. The second character, if present, can be any value 0–9. The square brackets ([ ]) indicate the possible range of characters and the question mark (?) indicates that the value is optional; that is, it may or may not be present. The third character is required; therefore, there is no question mark. However, the value can still be any number 0–9.

You can build your own regular expressions by experimenting with the default expressions. You can modify the default expressions to fine-tune your data searches or to create your own expressions.

Visit the AccessData website, www.accessdata.com, to find a technical document on Regular Expressions.

Creating Custom Regular Expressions

Create your own customized regular expressions using the following list of common operators

Common Regular Expression Operators

Operator	Description
.	A period matches any character.
+	Matches the preceding sub-expression one or more times. For example, “ba+” will find all instances of “ba,” “baa,” “baaa,” and so forth; but it will not find “b.”
$	Matches the end of a line.
*	Matches the preceding sub-expression zero or more times. For example, “ba*” will find all instances of “b,” “ba,” “baa,” “baaa,” and so forth.
?	Matches the preceding sub-expression zero or one times.
[ ]	Matches any single value within the square brackets. For example, “ab[xyz]” will find “abx,” “aby,” and “abz.”
-	A hyphen (-) specifies ranges of characters within the brackets. For example, “ab[0-3]” will find “ab0,” “ab1,” “ab2,” and “ab3.” You can also specify case specific ranges such as [a-r], or [B-M].
”	(Back quote) Starts the search at the beginning of a file.
‘	(Single quote or apostrophe) Starts the search at the end of a file.
\<	Matches the beginning of a word. In other words, the next character in any search hit must immediately follow a non-word character.
\>	Matches the end of a word. In other words, the last character in any search hit must be immediately followed by a non-word character.
|	Matches the sub-expression on either the left or the right. For example, A|u requires that the next character in a search hit be “A” or “u.”
\b	Positions the cursor between characters and spaces.
\B	Matches anything not at a word boundary. For example, will find Bob in the name Bobby.
\d	Matches any single decimal digit.
\l	Matches any lowercase letter.
\n	Matches a new line.
\r	Matches a return.
\s	Matches any whitespace character such as a space or a tab.
\t	Matches a tab.
\u	Matches any uppercase letter.
\w	Matches any whole character [a-z A-Z 0-9].
^	Matches the start of a line.

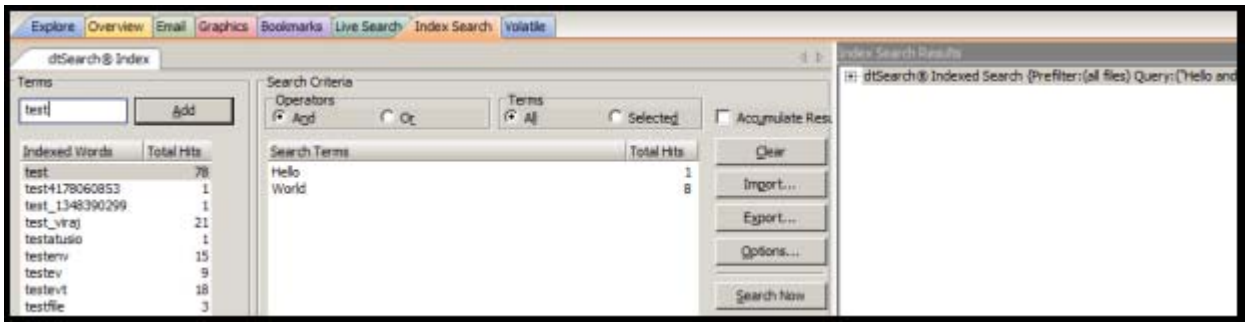
Common Regular Expression Operators (Continued)

Operator	Description
[[:alpha:]]	Matches any alpha character (short for the [a-z A-Z] operator).
[[:alnum:]]	Matches any alpha numerical character (short for the [a-z A-Z 0-9] operator).
[[:blank:]]	Matches any whitespace, except for line separators.
{*n*,*m*}	Matches the preceding sub-expression at least *n* (**number**) times, but no more than *m* ***(*****maximum*****)*** times.

Chapter 27

Searching Evidence with Index Search

Searching evidence for information pertaining to a case can be one of the most crucial steps in the examination. Index Search gives instantaneous results, and Live Search supports modes like text and hexadecimal. Search results are viewed from the *File List* and *File Contents* views in the *Search* tab.



This chapter details the use of the Index Search feature. It includes the following topics

- Conducting an Index Search (page 388)
- Using Search Terms (page 389)
- Defining Search Criteria (page 391)
- Exporting and Importing Index Search Terms (page 391)
- Selecting Index Search Options (page 392)
- Viewing Index Search Results (page 393)
- Using dtSearch Regular Expressions (page 394)
- Documenting Search Results (page 400)
- Using Copy Special to Document Search Results (page 401)
- Bookmarking Search Results (page 402)

Conducting an Index Search

The Index Search uses the index to find the search term. Evidence items may be indexed when they are first added to the case or at a later time. Whenever possible, AccessData recommends indexing a case before beginning analysis.

Index searches are instantaneous. In addition, in the Index Search Results List, the offset of the data in the hit is no longer listed in the hit. You will see it when you look at the hit file in Hex view.

Running an Index search on large files or Index Searches resulting in a large number of hits may make the scroll bar appear not to work. However, it will return when the search is complete. For more information about indexing an evidence item, see Indexing a Case (page 88).

The Search Criteria pane shows a cumulative total of all listed or all selected terms, based on the **And** or the **Or** operator. The cumulative total displays at the bottom of the Search Terms list. This functionality has been added to match the way the Search Terms list functioned in previous versions.

Select none, one, several, or all search terms from the list, click either **And** or **Or**, then click either **All** or **Selected** to see cumulative results. You can see this feature at work in the figure below.

Important: If you start an index search and then refresh the interface before the search finishes, the search will cancel and restart. This will cause a sizeable delay when searching in large or very large cases.

The Index contains all discrete words or number strings found in both the allocated and unallocated space in the case evidence.

You can configure how special characters, spaces and symbols are indexed. This is not done by default, however. One benefit is that you can easily search on an exact email address using `username@isp` (the extension, such as COM or NET, is not included automatically because a period (.) is not indexed.

In addition to performing searches within the case, you can also use the index to export a word list to use as a source file for custom dictionaries to improve the likelihood of and speed of password recovery related to case files when using the Password Recovery Toolkit (PRTK). You can export the index by selecting *File* > *Export Word List*.

Note: Performing a search using Unicode only works with Live Search, not Index Search.

UTF encoded documents can be searched using dtSearch.

Note: dtSearch has been updated which changes some of the search functionality and results. The search is now filtering Windows and Linux executables (EXE, BIN, OCF, and ELF). This may reduce the number of search results and reduce certain items from being shown in the filtered text. For example, the text in a header of an application may include “This program cannot be run in DOS mode”. Because it is now filtered it will not longer show in Filtered text.

Using Search Terms

Type the word or term in the Search Term field. The term and terms like it appear in the Indexed Words column displaying the number of times that particular term was found in the data. Click *Add* or press **Enter** to place the term in the Search Terms list, or double-click the term in the indexed words column to add it to the Search Terms list.

Using Unicode Characters in Search Terms

You can search for Unicode characters when performing a search. For example, you can search for the ö character.

To add Unicode characters

1. Turn on your keyboard's Num Lock.
2. In in the *Terms* field, enter the Unicode.
   For example, do the following:
   2a. Press and hold down the ALT key.
   2b. Using the numeric keypad only, type 148.
   2c. Release the ALT key and the character is entered.

Note: For Windows 7 and earlier you can use a 3-digit unicode number. For Windows 8 and higher you must use a 4-digit number. See http://support.microsoft.com/kb/315684/en-us.

Expanding Search Terms

When performing an Index Search, you can use the Term Browser to build a search using terms that are related to one or more keywords. You then select which words you want to include in the search.

To expand terms, a third-party lexical database called WordNet ® is used. When you expand terms, you can use the following lists: Synonyms, Related, Specific, General.

For example, you may start with a keyword of "delete." By using the Term Browser, it will suggest *synonyms*, such as "erase" and "cancel". It will also suggest *related terms*, such as "cut," "deletion," and "excision". It will also suggest *general related* terms, such as "censor," "remove," "take," and "withdraw." It will also suggest *specific related* terms, such as "strike," "excise," "scratch," and "expunge". You can select which of those words to include in your search.

The first time that you use this feature, the WordNet dictionary must be initialized. This is a one-time event and can take 5-15 minutes for it to complete. You are prompted before the initialization begins.

To search for terms using related words

1. In the *Examiner,* click **Index Search**.
2. Enter one or more keywords to the search terms.
3. Select one or more search terms that you want to expand.

4. Click **Expand Terms**.

   A list of synonyms is generated.

   To add other related words, select the **Include Related**, **Include Specific**, and **Include General** check boxes.

5. You can add terms to the term list, separated by a comma, and click **Expand**.
6. Select the words that you want to include in the search.
7. To build a search including the words that you selected, click **Add to Search**.

Defining Search Criteria

Refine a search even more by using the Boolean operators AND and OR. You can specify the terms to use in an index search by selecting specific entries, or by searching against all entries.

You can also use the NOT operator to force the search criteria to exclude terms. To do this, in the *Index Search* tab, in the *Terms* field, type NOT before the term that you want to exclude from the search criteria and then click **Add**.

For example, if you do not want to include files with the term “apple” in your search, enter **NOT apple** into the search criteria.

The Search Terms list now shows you a cumulative total for the search terms, individually, combined, or total. You can use the operators All and Selected to see more specific results. This is helpful when refining lists and terms to limit the results to a manageable number.

You can import a list of search terms to save having to type them multiple times. This is especially helpful when the list is long, or the terms are complex. When you create a search terms document, each term begins on a new line, and is followed immediately by a hard return. Save the file in TXT format in any text editor and save it for future use.

Important: When creating your search criteria, try to focus your search to bring up the smallest number of meaningful hits per search.

Exporting and Importing Index Search Terms

You can export a list of search terms you have added to the list of search terms to save for later use.

To export a set of search terms

1. Highlight the search terms to export to a file.
2. Click **Export**.
3. Provide a filename and location for the file (the TXT extension is added automatically).
4. Click **Save**.

To import a saved search terms file

1. Click **Import** to import a set of search terms.
2. Select the search terms file you previously saved.
3. Click **Open**.

Note: An imported term cannot be edited, except to delete a term and re-add it to your satisfaction.

Selecting Index Search Options

To refine an index search, from the Index Search tab, in the Search Criteria area click **Options**.

Important: The Search Options, *Stemming*, *Phonic*, and *Synonym* cannot be combined. You may choose only one at a time.

Index Search Options	
Stemming	Words that contain the same root, such as *raise* and *raising*.
Phonic	Words that sound the same, such as *raise* and *raze*.
Synonym	Words that have similar meanings, such as *raise* and *lift*.

Index Result Options	
Max Files to List	Maximum number of files with hits that are to be listed in the results field. You can change this maximum number in the field. Searches limited in this way will be indicated by an asterisk (*) and the text “(files may be limited by “Max files to list” option)” which may be cut off if the file name exceeds the allowed line length. The maximum number of possible files with hits per search is 65,535. If you exceed this limit, the remaining hits will be truncated, and your search results will be unreliable. Narrow your search to limit the number of files with hits. **Note:** Limiting the number of files to display does not work with some images. This is caused by dtSearch counting the chunks of files as individual files that are coming from the breaking of large unallocated space files into 10MB chunks. Since Those chunks are combined back into single files, the resulting file count will be less.
Max Hits per File	Maximum number of hits per file. You can change the maximum number in this field. Searches limited in this way will be indicated by an asterisk (*) and the text “(files may be limited by “Max hits per file” option)” which may be cut off if the file name and this text together exceed the allowed line length. The maximum number of possible hits per file is 10,000.
Max Words to Return	The maximum number of words to be returned by the search.

Files to Search	
All Files	Searches all the files in the case.
File Name Pattern	Limits the search to files that match the filename pattern. Operand characters can be used to fill-in for unknown characters. The asterisk (*) and question-mark (?) operands are the only special characters allowed in an index search. The pattern can include “?” to match any single character or “*” to match an unknown number of continuous characters. For example, if you set the filename pattern to “d?ugl*”, the search could return results from files named douglas, douglass, or druglord. To enter a filename pattern: ● Check the **File Name Pattern** box. ● In the field, enter the filename pattern. **Note:** Search by date range is now limited to be between Jan 1, 1970 and Dec 31, 3000.

Files to Search (Continued)

Files Saved Between	Beginning and ending dates for the time frame of the last time a file was saved. ● Check the **Files Saved Between** box. ● In the date fields, type the beginning and ending dates that you want to search between. **Note:** Search by date range is limited to be between Jan 1, 1970 and Dec 31, 3000.
Files Created Between	Beginning and ending dates for the time frame of the creation of a file on the suspect's system. ● Check the **Files Created Between** box. ● In the date fields, enter the beginning and ending dates that you want to search between. **Note:** Search by date range is now limited to be between Jan 1, 1970 and Dec 31, 3000.
File Size Between	Minimum and maximum file sizes, specified in bytes. ● Check the **File Size Between** box. ● In the size fields, enter the minimum and maximum file size in bytes that you want to search between.
Save as Default	Check this box to make your settings apply to all index searches.

Click *Search Now* when search criteria are prepared and you are ready to perform the search.

Viewing Index Search Results

Index Search results are returned instantaneously. The Index Search Results pane displays the results of your query in a tree-type view. The tree expands to show whether the resulting items were found in allocated or unallocated space. Further, when found in allocated space, the results are separated by file category. They are then sorted by relevancy, a percentage of the hits found per search term.

Using dtSearch Regular Expressions

You can use regular expression searching capabilities in the dtSearch index search tab. This functionality does not use RegEx++ that is used in the Live Search tab. dtSearch utilizes the TR1 (Technical Report 1) regular expressions.

Regular expressions in dtSearch provide a powerful syntax for searching for complicated patterns in text, such as one of several possible sequences of letters followed by a sequence of numbers. Regular expressions can also be used to express spelling variations of individual words. Regular expression patterns are arbitrary (i.e., supplied by the user dynamically) and cannot be pre-indexed.

Regular expression searching in dtSearch is limited to a single whole word. A regular expression included in the dtSearch box must be quoted and must begin with ##. An example of this is:

Apple and "##199[0-9]" - will find Apple and 1990 through 1999

Apple and "##19[0-9]+" - will find Apple and 190 through 199

However, if you want to look for Apple Pie, you cannot use "##app.*ie" since this is two words. Only letters and numbers are searchable. You cannot search for any of the non-indexed characters as defined in the I*ndex Search Settings* in the *Detailed Options* section of a case creation. Also, dtSearch does not store information about line breaks so any searches that are made that include the beginning of a line or the end of a line will not work.

Search considerations using the wildcard character "*" in a regular expression does have an effect on search speed: the closer to the front of a word the expression is, the more it will slow searching. "Appl.*" will be nearly as fast as "Apple", while ".*pple" will be much slower.

Note: Advanced searching for Social Security Numbers and Credit Card Numbers and other number patterns can be achieved, however modifications to the dtSearch engine must be made before processing the case. For more details, see Advanced Searching on page 7 of this paper.?

For more information, see:

- Regular Expressions - dtSearch Support. http://support.dtsearch.com/webhelp/dtsearch/regular_.htm
- MSDN: TR1 Regular Expressions. http://msdn.microsoft.com/en-us/library/bb982727.aspx

TR1 Regular Expressions For Text Patterns

Element Terms

Characters and target sequences are referred to as an Element and can be one of the following:

- A literal character typed as the actual letter or number (a or 1).
- A '.' (period) is any single character.
- An '*' (asterisk) is a wildcard character.
- (a) is a capture group.
- \d is a decimal character.
- For hex searches, \xhh matches a hex entry (ie - \x0f).

- {2} is a repetition character.
- A ',' (comma) is a minimum character.
- (aa?) is a target sequence.
- An alternation character search is 'this|that'.
- A concatenation sequence is '(a){2,3}(b){2,3}(c)'.
- A back reference is '((a+)(b+))(c+)\3'.
- (?:subexpression) matches the sequence of characters in the target sequence that is matched by the patter between the delimiters.
- (?!:subexpression) matches any sequence of characters in the target sequence that does not match the pattern listed in the subexpression)
- A bracket or range expression of the form "[expr]", which matches a value or a range, similar to a "set" in the Live Pattern Search.

Examples:

- "##a" matches the target sequence "a" but does not match the target sequences "b", or "c", and so on.
- "##." matches a single character such as "a", "b", and "c",and so on.
- "##sal*" matches the target 'sale' and the target "salt' and so on.
- "##(a)" capture group, matches the target sequence "a" but does not match the target sequences "b", or "c", and so on.
- "##\d\d\d\d" matches the target sequence of four digits "1234".
- "##aa?" or {0,1} matches the target sequence of "aa" and the target sequence of "aaa".
- "##ab" matches the target sequence "ab."
- "##[b-z]" or range, matches the target sequences "b" and "c" but does not match the target sequences "a".
- "##tom|jerry" matches the target sequence of 'tom' or 'jerry'.
- "##\d{4}" or repetition, matches the target sequence of four digits "1234".
- "##(?:aa)" or target sequence, matches the target sequence of "aa" and the target sequence of "aaa", and so on.

Ordinary Character

By entering actual ASCII characters, the search will return that set of characters after the element(s) are entered. By entering ordinary characters, "##nick", you would find said characters. However, if you wanted to look for Nick Davis, you could not use "##nick davis" since this is two words.

Single "Any" Character and Wildcard

The use of the any character element can be used if a letter or letters may be different, such as difference in spelling (example 'marijuana' and 'marihuana'). The wildcard is used to find any combination of characters after an element is entered.

Examples:

- "##(a*)" matches the target sequence "a", the target sequence "aa", and so on.
- "##a*" matches the target sequence "a", the target sequence "aa", and so on.

- "##(a.)" matches the target sequence "aa", the target sequence "ab", but will not find the target sequence the target sequence "aaa".
- "##a." matches the target sequence "aa", the target sequence "ab", but will not find the target sequence the target sequence "aaa".
- "##.*ick" matches the target sequence "nick", the target sequence "click", and so on.
- "##mari.uana" matches the target sequence "marijuana" and the target sequence "marihuana".

Capture Group

A capture group marks its contents as a single unit in the regular expression and labels the target text that matches its contents. The label that is associated with each capture group is a number, which is determined by counting the opening parentheses that mark capture groups up to and including the opening parenthesis.

Examples:

- "##(ab)*" matches the target sequence "ab", the target sequence 'abab", and so on.
- "##(a+)(b+)" matches the target sequence "ab, the target sequence "aab", the target sequence "abb", and so on.
- "##ab+" matches the target sequence "abb" but does not match the target sequence "abab."
- "##(ab)+" matches the target sequence "abab" but does not match the target sequence "abb."
- "##((a+)(b+))(c+)" matches the target sequence "aabbbc" and associates capture group 1 with the subsequence "aabbb", capture group 2 with the subsequence "aa", capture group 3 with "bbb", and capture group 4 with the subsequence "c".

Repetition

Any element can be followed by a repetition count.

Examples:

- "##(a{2})" matches the target sequence "aa" but not the target sequence "a" or the target sequence "aaa".
- "##(a{2,})" matches the target sequence "aa", the target sequence "aaa", and so on, but does not match the target sequence "a".

A repetition count can also take the following form:

- "?" - Equivalent to "{0,1}".

Examples:

- "a?" matches the target sequence "" and the target sequence "a", but not the target sequence "aa".
- "##(aa?)(bbbb?)(c)" matches the target sequence "aabbbbc" and the target sequence "abbbc".

Decimal Character

You can locate any set of decimals by using the '\d" character element in the expression.

Examples:

- "##\d\d\d\d" matches the target sequence "1234".
- "##\d[3} matches the target sequence "123".

- "##\d{3}\d\d\d\d" matches the target sequence '1234567".
- Visa and "##\d{4}" will match any files that contain the word 'visa' and any four digits.

Alternation

A concatenated regular expression can be followed by the character '|' and another concatenated regular expression. Any number of concatenated regular expressions can be combined in this manner. The resulting expression matches any target sequence that matches one or more of the concatenated regular expressions.

Example:

- "##(nick|houston)" matches the target sequence "nick", or the target sequence "houston".

Concatenation

Regular expression elements, with or without repetition counts, can be concatenated to form longer regular expressions. The resulting expression matches a target sequence that is a concatenation of the sequences that are matched by the individual elements.

Examples:

- "##(a){2,3}(b){2,3}(c)" matches the target sequence "aabbc", the target sequence "aaabbbc".
- "##(\d{4}){4}" matches the target sequence of "1234123412341234" (16 digits - no spaces).

Back Reference

A back reference marks its contents as a single unit in the regular expression grammar and labels the target text that matches its contents. The label that is associated with each capture group is a number, which is determined by counting the opening parentheses that mark capture groups up to and including the opening parenthesis that marks the current capture group. A back reference is a backslash that is followed by a decimal value N. It matches the contents of the Nth *capture group*. The value of N must not be more than the number of capture groups that precede the back reference.

Example:

- "((a+)(b+))(c+)\3" matches the target sequence "aabbbcbbb". The back reference "\3" matches the text in the third capture group, that is, the "(b+)". It does not match the target sequence "aabbbcbb".
  - The first capture group is ((a+)(b+))
  - The second capture group is (a+)
  - The third capture group is (b+)
  - The fourth capture group is (c+)

Bracket or Character Range

A character range in a bracket expression adds all the characters in the range to the character set that is defined by the bracket expression. To create a character range, put the character '-' between the first and last characters in the range. Doing this puts into the set all characters that have a numeric value that is more than or equal to the numeric value of the first character, and less than or equal to the numeric value of the last character.

Examples:

- "[0-7]" represents the set of characters { '0', '1', '2', '3', '4', '5', '6', '7' }. It matches the target sequences "0", "1", and so on, but not "a".
- "[h-k]" represents the set of characters { 'h', 'i', 'j', 'k' }.
- "[0-24]" represents the set of characters {'0', '1', '2', '4' }.
- "[0-2]" represents the set of characters { '0', '1', '2' }.

An individual character in a bracket expression adds that character to the character set that is defined by the expression. If the bracket expression begins with a "^" then this defines that the expression will consider all characters except for those listed.

Examples:

- "[abc]" matches the target sequences "a", "b", or "c", but not the sequence "d".
- "[^abc]" matches the target sequence "d", but not the target sequences "a", "b", or "c".
- "[a^bc]" matches the target sequences "a", "b", "c", or "^", but not the target sequence "d".

TR1 Regular Expressions For Number Patterns

If order to achieve dtSearch capability in FTK for search strings such as Social Security Numbers, Credit Card Numbers, Employee Identification Numbers, Telephone Numbers, and so on, where a period or hyphen is present, certain steps must be done during the pre-processing phase of the case.

Note: NOTE: Currently, you cannot include search patterns with spaces.

Normal dtSearch strings for credit card numbers or social security numbers

The normal dtSearch wildcard string can be utilized as long as the hyphen is set to be indexed as a space:

- Social Security Numbers - === == ====
  - Returns "123-45-6789"
  - Will not return "123 45 6789"
- Credit Card Numbers (16 digits) - ==== ==== ==== ====
  - Returns "1234-1234-1234-1234"
  - Will not return "1234 1234 1234 1234"

Number Patterns

You can use dtSearch TR1 Regular Expression to find number patterns as you can in Live Searches for such things as Credit Card Numbers, Social Security Numbers, xxxxxxxx. Certain pre-processing options MUST be completed before this function will work.

Configuring Pre-Processing Options

If you to utilize the dtSearch TR1 Regular Expression functions for looking for number patterns, you must complete the following pre-processing options:

1. Start a new case.
2. Click **Custom** processing profile.
3. Click **Indexing Options** next to dtSearch Text Index.
4. On the *Indexing Options* dialog window set the following:
   - For Hyphen Treatments - set to Hyphen
   - In the Spaces section - remove the period
   - In the Spaces section - remove the left and right parenthesis
   - In the Letters section - click Add and in all 4 spaces, type a "." period and repeat for the left and right parenthesis, then click OK.
5. Process the case.

Examples of TR1 Regular Expressions for Number Patterns

- For Credit Card Numbers:
  - "##(\d{4}[\.\-])(\d{4}[\.\-])(\d{4}[\.\-])(\d{4})"

    The first three groups are composed of - (\d{4}[\.\-]). The expression is looking for four digits followed by a period, or hyphen. This group is repeated three times and followed by the group looking for the ending 4 digits.

    We can shorten that expression by writing it "##((\d{4})[\.\-]){3}(\d{4})".

    This will find 1234-5678-1234-5678 or 1234.5678.1234.5678
- For Social Security Numbers -
  - "##(\d{3}[\.\-])(\d{2}[\.\-])(\d{4})".
  - This will find 123-45-6789 or 123.45.6789
- For U.S. Telephone Numbers -
  - "##(\d[\-\.])?(\(?\d{3}[\-\.\)])?([\-\.]?\d{3}[\-\.])(\d{4})"

    This will find:

    567-8901

    234-567-8901

    1-234-567-8901

    (234)567-8901

    (234)-567-8901

    567.8901

    234.567.8901

    1.234.567.8901

    (234)567.8901

    (234).567.8901

Documenting Search Results

Once a search is refined and complete, it is often useful to document the results.

Right-click an item in the *Search Results* list to open the quick menu with the following options:

- *Create Bookmark:* Opens the *Create Bookmark* dialog. For more information on creating and using Bookmarks, see Using the Bookmarks Tab (page 371).
- *Copy to Clipboard:* Copies the selected data to the clipboard (buffer) where it can be copied to another Windows application, such as an Excel (2003 or earlier) spreadsheet.

  Note: The maximum number of lines of data that can be copied to the clipboard is 10,000.

- *Export to File:* Copies information to a file. Select the name and destination folder for the information file. Uses the same criteria as Copy to Clipboard.
- *Set Context Data Width:* Context data width is the number of characters that come before and after the search hit.
- *Delete All Search Results:* Use this to clear all search results from the Index Search Results pane.

Copy or Export Search Results

All Hits in Case	Saves all the current search terms' hits found from the entire case.
All Hits in Search	Saves all the search hits found in each search branch.
All Hits in Term	(Live search only) saves the instances of individual terms found from the list of search terms. For example, if a live search consisted of the list "black," "hole," "advent," and "horizon," this option would copy information on each of the terms individually.
All Hits in File	Records the instances of the search term in the selected file only.
All File Stats in Case	Creates a CSV file of all information requested in the case.
All File Stats in Search	Creates a CSV file of the information requested in the search.
All File Stats in Term	(Live search only) Creates a CSV file of the instances of individual terms found from the list of search terms.

After the information is copied to the clipboard, it can be pasted into a text editor or spreadsheet and saved. Choose **Export to File** to save the information directly to a file. Specify a filename and destination folder for the file, and then click **OK**

Search results can then be added to the case report as supplementary files.

Important: When exporting Index Search result hits to a spreadsheet file, the hits are exported as a CSV file in UTF-16LE data format. When opening in Excel, use the Text to Columns function to separate the Index Search hit values into columns.

Using Copy Special to Document Search Results

The Copy Special feature copies specific information about files to the clipboard.

Method 1 to copy information about the files in your search results

1. Click in the search results list.
2. From the menu bar, select *Edit* > *Copy Special*.

Method 2 to copy information about the files in your search results

1. Find that file highlighted in the File List view.
2. Right-click on the desired file.
3. Select **Copy Special**.
4. Choose the column settings template to use from the drop-down list. Click *Column Settings* to define a new column settings template.
   4a. Modify the column template in the Column Settings Manager. For more information on customizing column templates, see Customizing File List Columns (page 481).
   4b. Click **Apply** to return to the *Copy Special* dialog.
5. Select the customized column template if you created one.
6. Choose whether you want to include the header row in the file.
7. Under File List Items to Copy, select the option that best fits your needs:
   - **All Highlighted** to copy only the items currently highlighted in the list.
   - **All Checked** to copy all the checked files in the case.
   - **Currently Listed** to copy all currently listed items, but no others.
   - **All** to copy all items in the case.
8. The dialog states the number of files that your selection contains.
9. Click **OK**.

Bookmarking Search Results

To keep track of particular search results, add them to new or existing bookmarks. Search results in the file list can be selected and added to a newly-created bookmark, or added to an existing bookmark as with any other data.

To create a bookmark from the file list

1. Select the files you want to include in the bookmark.
2. Right-click any of the selected files and select **Create Bookmark**.
3. Complete the *Create New Bookmark* dialog.
4. Click **OK**.
   The bookmark appears in the *Bookmark* tab.

Chapter 28

Viewing System Information

About Viewing System Information

You can view system information that contains detailed information about disk images in an easy to read format. You can view several important pieces of information about the target computer and the users of that computer.

You can view this information in the *System Information* tab.

Not all attributes are available for all disk images, however, the possible attributes that you can see are:

- Applications
  - Prefetch
  - User Assist
  - Installed
- Network Information
  - Network Shares
  - Network Connections
  - Wireless Profiles
- Owner Information
- Recent Files
  - LNK
  - NT User
  - Shortcuts
- SAM Users
- USB Devices

For details about the attributes, see Available System Information Data (page 406).

Populating the Data in the System Information Tab

The *System Information* tab is not populated with data by default. You must extract data during processing.

To extract data and have it populated in the System Information tab

- ❖ You must do one of the following:
  - When adding disk images to a case, select the *Generate System Information* processing option. See Evidence Processing Options on page 82.
  - For an existing case, use the *Generate System Information* option in *Additional Analysis*. See Using Additional Analysis on page 135.

Viewing System Information

After you have processed a disk image, you can view the system information.

To view system information data

1. Open the Examiner and click the **System Information** tab.

   You can choose one image at a time to review in further detail. On the left hand side, there is a dropdown list of all of the images that have been processed into the case.
2. Select the disk image that you want to view.
3. Select the nodes that you want to view.

   A tree of available attributes from the disk appears in the *Categories* panel.

   On the right side of the tab, there are two panels which display additional information about the node you select on the left. The upper panel is titled *Items* and the lower panel is titled *Provenance*.

   The *Items* panel displays lists of the attributes found within the selected node. For example, when looking at the *Applications* node, you may want to review a list of applications frequently used by the users of the target machine. You can select the node *User Assist* under the *Applications* node. Once you select this node from the tree on the left, in the *Items* panel you see a list of all of the applications frequently used by the users of the target machine along with the user that used that application, the number of times that application had been run, and the last time the application was run.

   The *Item* list allows you to sort any column in either ascending or descending order to assist you in finding the information you need quickly.

   In the *Provenance* panel, you can find the location of the data selected from the *Items* panel. Using the previous example of frequently used applications, you may want to review an application used by a specific user. From the *Items* list, you select the application you are interested in, and in the *Provenance* panel, you see the location from the target machine from which this information was obtained.
4. (Optional) In the *Provenance* panel, you can select the object, right-click, and set a bookmark.

Exporting System Information Data

You can export the content in the *Sytem Information* tab into an XML file.

To export system information data

1. From the *File Menu*, choose **Export System Information**.
2. In the *Export System Information* window, choose **All images** or **Selected image**. If you are choosing a specific image, be sure the image for which you would like to export system information is listed and highlighted in the Disk Images area. Press **OK**.
3. A *Save As* window will open. Select the directory and enter a file name for the output file. Press **Save**.

Note: In order to export system information data, the image must have been processed with the *Generate System Information* processing option selected during *Add/Remove evidence*, and the image must actually contain system information.

Available System Information Data

This section contains information about the possible data available in the *System Information* tab. All of the data is collected from one or more sources, where a source can be a single file or a location within the file. Where possible, the complete source path is shown in the *Provenance* pane. Below are the details of the data available for each category and sub-category.

Possible data available in the System Information tab

Category	Sub-Category	Description
Application Data		
	Prefetch	Each time you turn on your computer, Windows keeps track of the way your computer starts and which programs you commonly open. Windows saves this information as a number of small files in the prefetch folder. The next time you turn on your computer, Windows refers to these files to help speed the start process. The prefetch folder is a subfolder of the Windows system folder. The prefetch folder is self-maintaining, and there's no need to delete it or empty its contents. If you empty the folder, Windows and your programs will take longer to open the next time you turn on your computer. For each prefetch (.PF) file, in the System Information tab displays the following information: ● Complete path to the application executable ● Number of times the application was run. ● Last time the application was run
	User Assist	UserAssist is a method used to populate a user's start menu with frequently used applications. This is achieved by maintaining a count of application use in each users NTUSER.DAT registry file at sub key: ● Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist For each UserAssist entry in the registry, the System Information tab displays the following information: ● Complete path to the application executable ● Number of times the application was run ● Last time the application was run

Possible data available in the System Information tab (Continued)

Category	Sub-Category	Description
	Installed	Applications installed on the Windows system are viewable via the Control Panel -> Programs and Features. By default the list doesn't show updates or system components unless the user selects to see them. The information can come from various places in the registry but the feature uses the HKLM\SOFTWARE registry file under the sub keys: ● Microsoft\Windows\CurrentVersion\Uninstall\ ● Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\ Service packs, hot fixes, updates, or system components are not reported. For each installed application, the System Information tab displays the following information: ● Application name ● Application publisher (if available) ● Path to installed application (if available) ● Date application was installed (if available) ● Size of application install base (if available) ● Application version (if available)
Network Data		
	Network Shares	A network share is a computer resource made available from one host to other hosts on a computer network. In this feature, it is specifically the networks that were accessed using the Universal Naming Convention (UNC). This information is stored in each user's NTUSER.DAT registry file at sub keys: ● Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\Map Network Drive MRU ● Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\RunMRU ● Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\MountPoints2 For each installed application, the System Information tab displays the following information: ● UNC Path ● Last connection time

Possible data available in the System Information tab (Continued)

Category	Sub-Category	Description
	Network Connections	A network connection provides connectivity between one computer and the Internet, a network, or another computer. In every case the connected to network has an identifying name. Network connections managed by Windows are stored in the HKLM\SOFTWARE registry file under the sub key: ● Microsoft\\Windows NT\\CurrentVersion\\NetworkList For each network connection, the System Information tab displays the following information: ● Profile name ● First time connecting to the network ● Most recent time connecting to the network ● Network name ● Network category (e.g. Domain, Private, Public) ● Gateway MAC address ● Whether it is a wireless network (This is only set if for sure it is a wireless network)
	Wireless Profiles	A wireless profile is a set of configuration parameters that allow a system to connect to a wireless access point. The profiles managed by Windows are stored in the file C:\ProgramData\Microsoft\Wlansvc\Profiles\Interfaces For each wireless profile, the System Information tab displays the following information: ● Profile name ● SSID ● Authentication (e.g. WPA2PSK, WPAPSK, etc.) ● Encryption (e.g. TKIP, AES, none, etc.)
Owner Information Data		This is basic data about the installed operating system and comes from the HKLM\SOFTWARE registry file under the sub key: ● Microsoft\\Windows NT\\CurrentVersion For each registry value, the System Information tab displays the following information: ● Name of the registry value ● The contents of the registry value
Recent Files Data		

Possible data available in the System Information tab (Continued)

Category	Sub-Category	Description
	NTUser	Many applications store recently used files in the user's NTUSER.DAT registry file. The specific applications that are extracted are from Microsoft Office and Adobe Acrobat. The following sub keys are examined: ● Software\Microsoft\Office ● Software\Adobe ● Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU ● Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU ● Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2 For each recently used file, the System Information tab displays the following information: ● Application name (i.e. Acrobat, Excel, PowerPoint, Word) ● Absolute path to the recent file
	LNK Files	LNK is a file extension for a shortcut file used by Microsoft Windows to point to an executable file. LNK stands for LiNK. Shortcut files are used as a direct link to an executable file, instead of having to navigate to the executable, LNK files are stored in each users' AppData\Roaming\Microsoft\Windows\Recent or Recent directory. For each LNK file, the System Information tab displays the following information: ● Absolute path to target file ● Date/Time the target file was created ● Date/Time the target file was last written to ● Date/Time the target file was last accessed
	Jump Lists	Jump Lists, new in Windows 7, take you right to the documents, pictures, songs, or web sites you turn to each day. To open a Jump List, just right-click a program button on the Windows 7 taskbar. (You can also get to Jump Lists by clicking the arrow next to the program name on the Start menu.) The files that support this feature are located in each users' AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations folder. For each LNK file inside each Jump List, the System Information tab displays the following information: ● Absolute path to target file ● Date/Time the target file was created ● Date/Time the target file was last written to ● Date/Time the target file was last accessed

Possible data available in the System Information tab (Continued)

Category	Sub-Category	Description
SAM Users Data		The Security Accounts Manager (SAM) HKLM\SAM registry file stores users' passwords in a hashed format either as a LAN hash or NT hash. To protect the file, Microsoft introduced the SYSKEY function so the on-disk copy of the SAM is partially encrypted with a key (usually referred to as the "SYSKEY"). For each user stored in the SAM registry, the System Information tab displays the following information: ● Name of the user ● SID ● Unencrypted current LAN hash ● Unencrypted previous LAN hash ● Unencrypted current NT hash ● Unencrypted previous NT hash
USB Devices		When USB devices are plugged into a computer for the first time, the Windows operating installs an appropriate driver and stores information about the device in the registry and the setupapi log file. On subsequent device connections, various registry keys are updated to reflect the last connection time. Details about each USB devices are stored in the following registry locations: ● HKLM\SOFTWARE\Microsoft\\Windows NT\\CurrentVersion\\EMDMgmt ● HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR ● HKLM\SYSTEM\CurrentControlSet\Enum\USB ● HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b} ● HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56308-b6bf-11d0-94f2-00a0c91efb8b} ● HKLM\SYSTEM\MountedDevices ● HKU\<user sid>\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2 For each USB device, the *System Information* tab displays the following information: ● Vendor name ● Vendor id ● Product name ● Product id ● Instance id (very similar to serial number) ● Revision ● First time device was connected ● Last time device was connected ● Last time a user mounted the device ● Drives the device was mounted to ● Volume labels

Chapter 29

Examining Volatile Data

This chapter includes the following topics

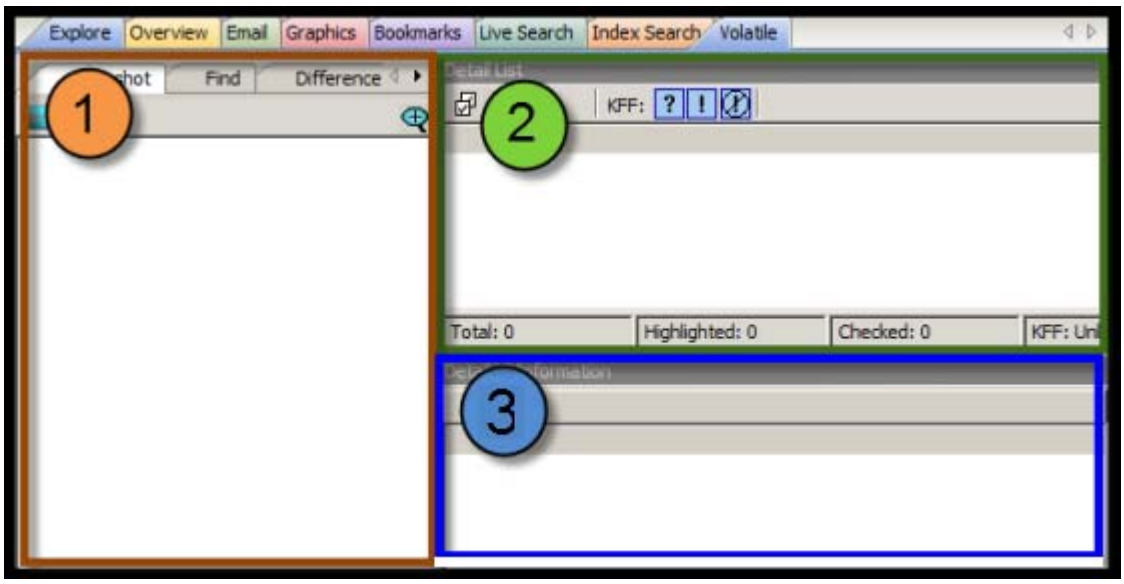
- Using the Volatile Tab (page 412)
- Understanding Memory (page 414)
- Viewing Memory Dump Data (page 415)
- Performing File Remediation from the Volatile Tab (page 417)
- Killing a Process (page 417)
- Wiping a File (page 418)
- Adding Hashes to KFF Library from the Volatile Tab (page 418)
- Adding Hashes to Fuzzy Hash Library from the Volatile Tab (page 419)
- Creating a Memory Dump File (page 419)

Using the Volatile Tab

The *Volatile* tab provides tools for viewing, finding, and comparing data gathered from the memory of live agent systems in your network. Other data acquired remotely, such as from a Mounted Image Drive or a Mounted Device is viewable from other tabs. The Volatile tab is specifically for remote memory data acquired as a memory dump. It can be added directly to a case upon acquisition, or saved as a dump file to be added to any case at a later time.

See Working with Live Evidence (page 144).

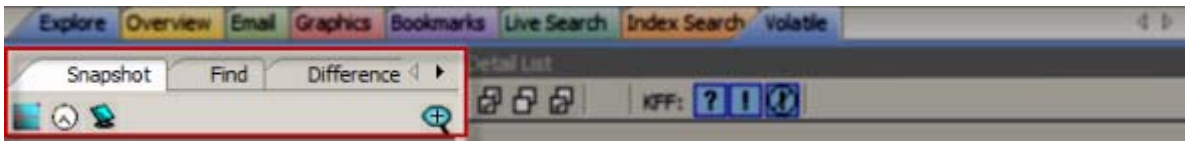
When you have acquired volatile (Memory) data as a dump file the resulting acquisition data is displayed in the *Volatile* tab.



There are three main areas in the Volatile tab:

1. Tabbed Data View
2. Detail List View
3. Detailed Information View

It is important to remember that the views relate clockwise. When an item is selected in the *Tabbed Data* view, the related information is displayed in the *Detail List* view. An item selected in the *Detail List* view will display relevant information in the *Detailed Information* view, within the data tab that relates to the type of item that is selected.



The *Tabbed Data* view has three tabs:

- Snapshot
- Find
- Difference

Each *Tabbed Data View* displays a summary of acquired volatile data.

Data View Sort Options

Button	Description
	Sort acquired volatile data by *Operation Type*, such as those selectable from the **Evidence > Add Remote Evidence > Selection Information** dialog box. Found on Snapshot, Find, and Difference tabs.
	Sort acquired volatile data by the *Time of Acquisition*, displayed in the local machine's time. Found on *Snapshot*, *Find*, and *Difference* tabs.
	Sort acquired volatile data by the *Source Machine or Agent*. Found on *Snapshot*, *Find*, and *Difference* tabs.
	Display saved comparisons. When a comparison of found data is done, the results can be saved and viewed later. Found only on the *Difference* tab
	Geolocation. This button on the Volatile tab that will launch Geolocation for volatile data. See Viewing Geolocation IP Locations Data on page 464.

The *Detail List View* provides information specific to the item currently selected in the Data View. The content of the Detail List changes as different items are selected.

The *Detailed Information View* shows more specific information about the item in the Data View, and its selected component in the Detail List view.

Understanding Memory

Memory can include the physical “sticks” of memory that we put into the machine, commonly referred to as physical memory. However, video cards, network cards, and various other devices use memory that the Operating System (OS) must be able to access in order for the devices to work properly. Both physical memory and device memory are organized by the OS in a linear address map. For 32-bit operating systems, the linear address map is naturally 4GB. Traditionally the OS will put physical memory at the bottom of this map and the device memory at the top.

When a system has a full 4GB of physical memory, using all 4GB wouldn’t leave any room to address the device memory.

Since the OS can’t function without access to the device memory, it simply doesn’t use all 4GB of physical memory. Evidence of this fact can be seen on the main Properties window of My Computer. If you have a 32-bit Windows XP system with 4GB of physical memory, you may notice that the Properties window will show that you have only 3.25GB of physical RAM. That limitation allows for addressing of devices within the 4GB address space.

Most acquisition products check how much physical memory is **available** (4GB using our example above), open a handle to the OS’s memory map (referred to as \Device\PhysicalMemory) and start reading, one page at a time. Thus, in an attempt to read all of the physical memory, what they are actually reading is the OS’s linear address map of both physical and device memory. However, some device memory is not meant to be read and the simple act of reading it could cause system instability. In fact, if the OS is 64-bit, this algorithm would miss the physical memory that was placed beyond the 4GB range.

The approach AccessData takes is to query the OS’s memory map for the regions that correspond to physical memory and only acquire those regions - filling the other regions with zeros. This method not only avoids any issue with system instability but also guarantees that it acquires all the physical memory that the OS is able to use — the memory that anyone would normally be interested in.

Viewing Memory Dump Data

A Memory Dump file includes all the Processes, DLLs, Sockets, Drivers, Open Handles, Processors, System Descriptor Tables and Devices in use at the time of the acquisition. The Volatile tab provides a view of all this data by type.

Right-click on any dump file in the Snapshot view to choose View Memory or Search Memory.

Viewing Hidden Processes

Hidden processes are automatically detected. There is no way to disable or turn off this feature. The detection compares a list of processes in memory to the operating systems's processes list to determine whether any running processes do not belong. These are the processes that are highlighted in yellow.

Hidden processes, when detected in a Memory Dump file, and found only in the Process List. Click on a dump file in the Process List, then scroll down the Detail List to locate any lines highlighted in yellow.

Click on a yellow-highlighted line in the Detail List to display related information in the Detailed Information list. Scroll across the columns list to see all the data.

Viewing Input/Output Request Packet Data

Input/Output Request Packet (IRP) data, also known as memory hooks, when detected in a memory dump file, are indicated in the *Snapshot* view by a yellow warning indicator. Memory hooks can be used for both legitimate and non-legitimate purposes.

In the *Detail* list, the items that contain memory hooks are highlighted in pink. Click on a pink-highlighted item to open that item in the *Detailed Information* view. The *IRP* tab shows the items and properties that are related to the IRP data that was detected. This data does not identify whether the IRP was bad or good, only that it was there, so you can determine its nature.

Tabs in the *Detailed Information* list provide additional related data for the selected data type. Some data types have several tabbed pages, and some have only a few. Each tabbed page contains different information related to the selected item, and each displays properties specific to the tabbed page for that information type. The property column headings are sortable to make it easier to locate critical information.

In addition to the IRP data view, access is provided to Service Descriptor Tables (SDT), and System Service Descriptor Tables (SSDT).

Up to four SSDT tables are available. The four tabs are placeholders only; their existence does not indicate nor guarantee they will be populated. Notice that the names of the populated tables' tabs are longer than those that are not populated. Only the data that is found in the evidence can be displayed.

Viewing Virtual Address Descriptor (VAD) Data

In the Windows operating system, every object opened by a program (example files, screens, sections of memory, etc.) is assigned a handle that the process in which the program is running can use. These handles are stored in a table that is managed by the process. This table is called the virtual address descriptor table (VAD).

A single process normally contains many VADs. Each VAD describes a range of virtual pages and tells the Memory Manager what those virtual pages represent. For example, a typical process will consist of an executable image (the program) and a set of dynamic link libraries (DLLs) that are used within that process, as well as data that is unique to the program. Each of these separate items exists somewhere within the address space of the program.

When each component is first loaded into the address space, the Memory Manager creates a new VAD entry for each such range of addresses. These VAD entries are in turn linked together in a binary tree that optimizes access to the most recently accessed VAD. This representation makes it is easy to describe a sparse address space using a tree of VADs, it is fast to find entries within the VAD tree, and it is easy to reorganize VAD entries as necessary.

Investigating the VAD tree lets you view resources allocated by a program. The VAD tree constantly changes during execution of a program. Each time the VAD tree is read, the results are different.

To view Virtual Address Descriptor (VAD) Data

1. In the *Examiner*, select the *Volatile* tab.
2. In the *Snapshot* tab, expand **Process List**.
3. Expand the date of the snapshot.
4. Select the computer name.
5. In the upper-right pane, under *Detail List*, select a process.
6. In the lower-right pane, under *Detailed Information*, click the **VAD** tab.
7. The Virtual Address Descriptor (VAD) information is displayed in the *Detailed Information* pane.

Performing File Remediation from the Volatile Tab

Certain file remediation tasks are available for specific data types in the Volatile tab. After a remote volatile data acquisition is completed, click to expand the data type in the Snapshot tabbed view, then right-click on the item in the Detail List to choose from the available file remediation options.

Volatile Tab File Remediation Options

Volatile Data Type	Kill Process	Wipe File	Add Hashes to KFF Lib	Add Hashes to Fuzzy Lib	Dump
Process List	X	X	X	X	X
DLL List	--	--	X	X	X
Sockets	--	--	--	--	--
Driver List	--	--	X	X	
Open Handles	--	--	--	--	--
Processors	--	--	--	--	--
System Descriptor Table	--	--	--	--	--
Devices	--	--	--	--	--

Killing a Process

Kill Process ends a process running on the remote computer the data was acquired from.

To kill a process

1. In the *Snapshot* view, click and expand the *Process List*.
2. In the *Detail List*, highlight or mark the check boxes of the processes to be killed.
3. Right-click in the Detail List and select **Kill Process**.
4. In the *Select Source* dialog box, select either **Highlighted Detail List items**, or **Checked items**.
5. Click **OK**.

Wiping a File

Wipe File completely removes a file from the remote computer the file was acquired from.

To wipe a file

1. In the *Snapshot* view, click and expand the *Process List*.
2. In the *Detail List*, highlight or mark the check boxes of the file to be wiped.
3. Right-click in the *Detail List* and select **Wipe File**.
4. In the **Select Source** dialog box, select either **Highlighted Detail List item**s, or **Checked items**.
5. Click **OK**.

Adding Hashes to KFF Library from the Volatile Tab

Hashes can be added directly to the KFF Library directly from the Volatile tab.

To add hashes to the KFF Library

1. In the *Detail List*, highlight or mark the check boxes of the hashes to add to the KFF Library.
2. Right-click in the *Detail List*, and click **Add Hashes to KFF**.
3. Provide a name for the set.
4. Click **Add all hashes** to add the hashes of all displayed items, or **Add only checked hashes** in the current Detail List.
5. Select either **Alert** or **Ignore**.
6. Choose whether or not to **Activate in [the current] case**.
7. Click **OK**.

Adding Hashes to Fuzzy Hash Library from the Volatile Tab

Hashes can be added directly to the Fuzzy Hash Library directly from the Volatile tab.

To add hashes to the Fuzzy Hash Library

1. In the Detail List, highlight or mark the check boxes of the file(s) hashes to add to the Fuzzy Hash Library.
2. Right-click in the Detail List, and click **Add Hashes to Fuzzy**.
3. Provide a name for the set.
4. Click **Add all hashes** to add the hashes of all displayed items, or **Add only checked hashes** in the current Detail List.
5. Select either **Alert** or **Ignore**.
6. Assign a *Threshold Value*.
7. Choose whether or not to **Activate in [the current] case**.
8. Click **OK**.

Creating a Memory Dump File

A dump file can be created and added to the case directly from the Volatile tab.

To create a Dump file

1. In the *Snapshot* view, click and expand the *Process List* or the DLL List.
2. In the *Detail List*, highlight or mark the check boxes of the files to be dumped.
3. Right-click in the Detail List and select **Dump to file**.
4. In the *Dump a file* dialog box, mark **Include DLLs with processes**, and/or **Include parent process with DLLs**.
5. Browse to and select a destination path for the dump file.
6. Click **OK**.

Chapter 30

Analyzing Document Content

Depending on your license, you can analyze the content of documents in your evidence in the following ways:

- Using Document Content Analysis (page 424)
- Performing Cluster Analysis (page 426)
- Using Entity Extraction (page 420)

Using Entity Extraction

About Entity Extraction

You can extract entity data from the content of files in your evidence and then view those entities.

You can extract the following types of entity data:

- Credit Card Numbers
- Phone Numbers
- Social Security Numbers

The data that is extracted is from the body of documents, not the meta data.

Using entity extraction is a two-step process:

1. Process the data with the *Entity Extraction* processing options enabled.
   You can select which types of data to extract.
2. View the extracted entities in the *Examiner*.

The following table provides details of the type of data that is identified and extracted:

Entity Extraction Details

Type	Examples
Credit Card Numbers	Numbers in the following formats will be extracted as credit card numbers:

Entity Extraction Details

Type		Examples
	16-digit numbers used by VISA, MasterCard, and Discover in the following formats.	For example, ● 1234-5678-9012-3456 (segmented by dashes) ● 1234 5678 9012 3456 (segmented by spaces) Not: ● 1234567890123456 (no segments) ● 12345678-90123456 (other segments)
	15-digit numbers used by American Express in the following formats.	For example, ● 1234-5678-9012-345 (segmented by dashes) ● 1234 5678 9012 345 (segmented by spaces)
		Notes: Other formats, such as 14-digit Diners Club numbers, will not be extracted as credit card numbers
Phone Numbers	Numbers in the following formats will be extracted as phone numbers:	
	Standard 7-digit	For example: ● 123-4567 ● 123.4567 ● 123 4567 Not: 1234567 (not segmented)
	Standard 10-digit	For example: ● (123)456-7890 ● (123)456 7890 ● (123) 456-7809 ● (123) 456.7809 ● +1 (123) 456.7809 ● 123 456 7809 Not 1234567890 (not segmented) Note: A leading 1, for long-distance or 001 for international, is not included in the extraction, however, a +1 is.

Entity Extraction Details

Type		Examples
	International	Some international formats are extracted, for example, ● +12-34-567-8901 ● +12 34 567 8901 ● +12-34-5678-9012 ● +12 34 5678 9012 Not 12345678901 (not segmented) Other international formats are not extracted, for example, ● 123-45678 ● (10) 69445464 ● 07700 954 321 ● (0295) 416,72,16
		Notes: Be aware that you may get some false positives. For example, a credit number 5105-1051-051-5100 may also be extracted as the phone number 510-5100.
Social Security Numbers	Numbers in the following formats will be extracted as Social Security Numbers:	
		● 123-45-6789 (segmented by dashes) ● 123 45 6789 (segmented by spaces) The following will not be extracted as Social Security Numbers: ● 123456789 (not segmented) ● 12345-6789 (other segments)

Enabling Entity Extraction

To enable entity extracting processing options:

1. You can enable entity extracting processing options at one of two times:
   - When creating a case or adding new evidence and configuring processing options.
     See Evidence Processing Options on page 82.
   - When running Additional Analysis on existing evidence.
     See Using Additional Analysis on page 135.

Viewing Entity Extraction Data

To view extracted entity data

1. In the *Examiner*, click the **Overview** tab.
2. Expand the *Document Content* node.
3. Expand a *Document Content* type, such as *Credit Card Numbers* or *Phone Numbers*.
4. Click an item to show the file in the *File List* that contains the extracted data.

Using Document Content Analysis

You can use Document Content Analysis to group document data together for quicker review.

Note: If you activated Document Content Analysis as an Evidence Processing option when you created the project, Document Content Analysis will automatically run after processing data and will not need to be run manually.

To perform Document Content Analysis on a new case

1. From *Case Manager*, click **Manage > Evidence Processing Profiles**.
2. In the *Manage Evidence Processing Profiles* dialog, create a new profile or edit an existing profile.

   See Configuring Default Processing Options for a Case on page 76.

   See Using Processing Profiles on page 77.
3. From the *Detailed Options* dialog, click the *Evidence Processing* tab from the left menu and select **Document Content Analysis**.
4. (Optional) Click **DCA Options** and change the *Analysis Threshold*, if needed, and click **OK**.
   - *Analysis Threshold* — Sets the level of similarity (in a percentage) that is required for documents to be considered related or near duplicates. The higher the percentage, the more similar the documents need to be in order to be considered similar.
5. Click **Save As** and follow the screens to save and/or replace the profile.

To perform Document Content Analysis on an existing case

1. In *Evidence Explorer*, click **Evidence > Add/Remove**.
2. From the *Manage Evidence* dialog, highlight the evidence you want to process using Document Content Analysis.
3. Click **Refinement Options**.
4. Select **Document Content Analysis** and change the DCA options, if needed. See Evidence Processing Options on page 82.

Filtering Documents by Document Content Analysis

Documents processed with Document Content Analysis can be filtered by the content of the documents in the evidence. The Cluster Topic container is created in Evidence Explorer in the *Overview* > *Case Overview* tab and is created from data processed with Document Content Analysis. Data included in the Cluster Topic container is taken from documents, including Word documents, text documents, and PDF documents.

In order for the application to filter the data and display the Cluster Topic container, the following must occur:

- Prerequisites for Cluster Topic (page 425)
- How Document Content Analysis Works (page 425)
- Filtering with Cluster Topic (page 425)
- Considerations of Cluster Topic (page 425)

Prerequisites for Cluster Topic

Before the Cluster Topic container can be created, the data in the project must be processed by Document Content Analysis. The data is processed automatically when Document Content Analysis is selected in the Evidence Processing options or you can process the data manually by selecting **Document Content Analysis** in the *Refinement Options* > *Evidence Processing* dialog.

Evidence Processing Options (page 82)

Configuring Evidence Refinement (Advanced) Options (page 100)

How Document Content Analysis Works

The application uses an algorithm to cluster the data. The algorithm accomplishes this by creating an initial set of cluster centers called pivots. The pivots are created by sampling documents that are dissimilar in content. For example, a pivot may be created by sampling one document that may contain information about children's books and sampling another document that may contain information about an oil drilling operation in the Arctic. Once this initial set of pivots is created, the algorithm examines the entire data set to locate documents that contain content that might match the pivot's perimeters. The algorithm continues to create pivots and clusters documents around the pivots. As more data is added to the project and processed, the algorithm uses the additional data to create more clusters.

Word frequency or occurrence count is used by the algorithm to determine the importance of content within the data set. Noise words that are excluded from Document Content Analysis are also not included in the Cluster Topic pivots or clusters.

Filtering with Cluster Topic

Once data has been processed by Document Content Analysis and categories are created under the Cluster Topic container, you can view the data in the *Overview* > *File List*.

Using the Overview Tab (page 306)

Cluster Topic Container (page 309)

The topics of the categories available are terms created during the Document Content Analysis. Documents containing these terms are included in the category and are displayed in the *File List* when selected. Categories are comprised of two word phrases that occur in the documents. This is to make the category more legible.

The UNCLUSTERED category contains any documents that are not included under a *Cluster Topic* Container.

Considerations of Cluster Topic

You need to aware the following considerations when examining the Cluster Topic categories:

- Not all data will be grouped into categories at once. The application creates categories in an incremental fashion in order to return results as quickly as possible. Since the application is continually creating categories, the Cluster Topic container is continually updated.
- Duplicate documents are grouped together as they match a specific category. However, if a category is particularly large, duplicate documents may not be included as part of any category. This is to avoid

performance issues. You can examine any duplicate documents or any documents not included in a category by highlighting the *UNCLUSTERED* category of the *Cluster Topic* container.

- Cluster Topic results can vary when performed on different databases and/or different computers. This is due to the analytic behavior of the Document Content Analysis process. Since limits have been set on the algorithm to allow for efficient collection of data, large amounts of content can thus produce varying results.

Performing Cluster Analysis

Depending on the license you own (an AD Lab license or a AD Summation license), you can perform an analysis of files to determine related documents and email threads. If there are files that are similar, one document is identified as the pivot, and then the other related files are given a score that shows how closely they are related to the Pivot. If a score is 100, it is a perfect match.

Note: With an FTK, FTK PRO, or AD Enterprise license, you can perform Cluster Analysis on a documents only using the Document Content Analysis feature.
See Using Document Content Analysis on page 424.

You perform the Cluster Analysis by enabling the Cluster Analysis processing option.

See Identifying Processing-Generated Data on page 333.

See Relating Generated Files to Original Files on page 333.

When you enable Cluster Analysis, you have the following options:

- Document Types to process - You can select to process the following file types:
  - Documents
  - Presentation
  - Spreadsheets
  - Email
- Similarity Threshold - Determines the level of similarity required for documents to be considered related or near duplicates.

After processing is complete, you can add the *Review Set Pivot* and the *Distance to Pivot* columns in the File List in the Examiner. You will also use the standard *Item #* column to identify the Pivot file.

See Managing Columns on page 481.

To Perform Cluster Analysis

1. When either adding evidence to a case or performing Additional Analysis, access the processing options.
   See Selecting Lab/eDiscovery Options on page 104.
   See Using Additional Analysis on page 135.
2. Select the option for **Cluster Analysis**.
3. Click **NDA Options**.
4. Select the document types to process and the similarity threshold.
5. Process your data.

To view Cluster Analysis data using columns

1. In the examiner, view the file types that you selected.
2. Click the Column Settings icon.
   See Managing Columns on page 481.
3. Either create a new column template or edit an existing one.
4. Add the following columns to the template.
   - Item #
   - Review Set Pivot
   - Distance to Pivot
5. Click **OK.**
6. Select the template name you just configured.
7. Click **Apply.**
   This applies the template to the File List.
8. Click **Close.**
   The Review Set Pivot shows the Item # of the Pivot file, or the file that other files are compared to.
   If a file was identified as being a near duplicate, it will show a Distance to Pivot score. A perfect match has a score of 100.

Words Excluded from Cluster Analysis Processing

Noise words, such as if and or, are excluded from Cluster Analysis processing. The following words are excluded in the processing:

a, able, about, across, after, ain't, all, almost, also, am, among, an, and, any, are, aren't, as, at, be, because, been, but, by, can, can't, cannot, could, could've, couldn't, dear, did, didn't, do, does, doesn't, don't, either, else, ever, every, for, from, get, got, had, hadn't, has, hasn't, have, haven't, he, her, hers, him, his, how, however, i, if, in, into, is, isn't, it, it's, its, just, least, let, like, likely, may, me, might, most, must, my, neither, no, nor, not, of, off, often, on, only, or, other, our, own, rather, said, say, says, she, should, shouldn't, since, so, some, than, that, the, their, them, then, there, these, they, they're, this, tis, to, too, twas, us, wants, was, wasn't, we, we're, we've, were, weren't, what, when, where, which, while, who, whom, why, will, with, would, would've, wouldn't, yet, you, you'd, you'll, you're, you've, your.

Chapter 31

Using Visualization

About Visualization

Visualization is a component that provides a graphical interface to enhance understanding and analysis of files and emails in a case. You view data based on file and email dates. Visualization provides dashboards with chats and lists that quickly show information about the data in the specified date range. Visualization helps you identify files and emails that you label and bookmark as part of your investigation.

Note: The Visualization feature is available as an add-on license. Please contact your AccessData sales representative for more information.

Visualization can only display data that has an associated date. If a file or an email does not contain a valid Created, Modified, Last Accessed, Sent or Received date, it is not displayed. For example, carved files do not have an associated date so they are not displayed in Visualization.

You can also take screen captures of the Visualization pages to have a record of the data.

Visualization supports the following data types:

- File Data: You can view file data from either the *Explore* tab or the *Overview* tab in the *Examiner* interface.
  For more information see Visualizing File Data (page 435).
- Email Data: You can view email data from the *Email* tab in the *Examiner* interface.
  For more information see Visualizing Email Data (page 442).
- Internet Browser History: You can view internet browser history data.
  For more information see Visualizing Internet Browser History Data (page 454).

Visualization also has the following components:

- Using Visualization Heatmap (page 455)
- Using Visualization Social Analyzer (page 457)
- Using Visualization Geolocation (page 463)

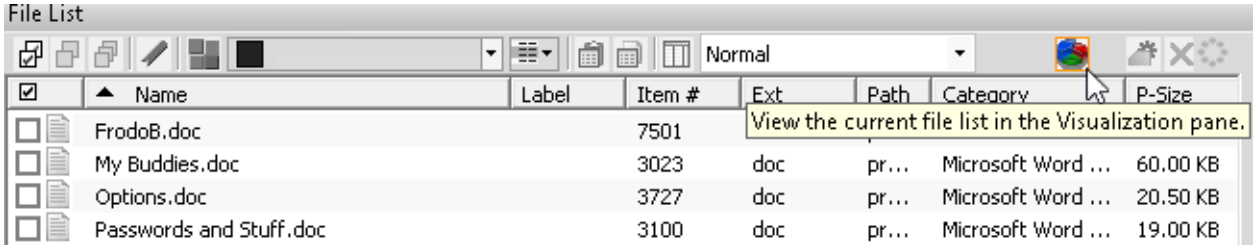
Launching Visualization

To launch visualization

1. Use the *Explore*, *Overview*, or *Email* tabs to specify a set of data.

   For example, in the *Overview* tab, you can view everything under *File Extension* or drill down to just DOC files.

2. When you have specified the data that you want to view in the Visualization pane, click the following pie chart icon:



   The data that you have displayed in the *File List* pane is the data that you can send to the visualization module.

   The visualization module opens in a separate window from the *Examiner* that you can minimize, maximize, and select in the Windows task bar.

3. On the time line, specify the date range for the base time line that you want to view data for.

   See Setting the Base Time Line on page 433.

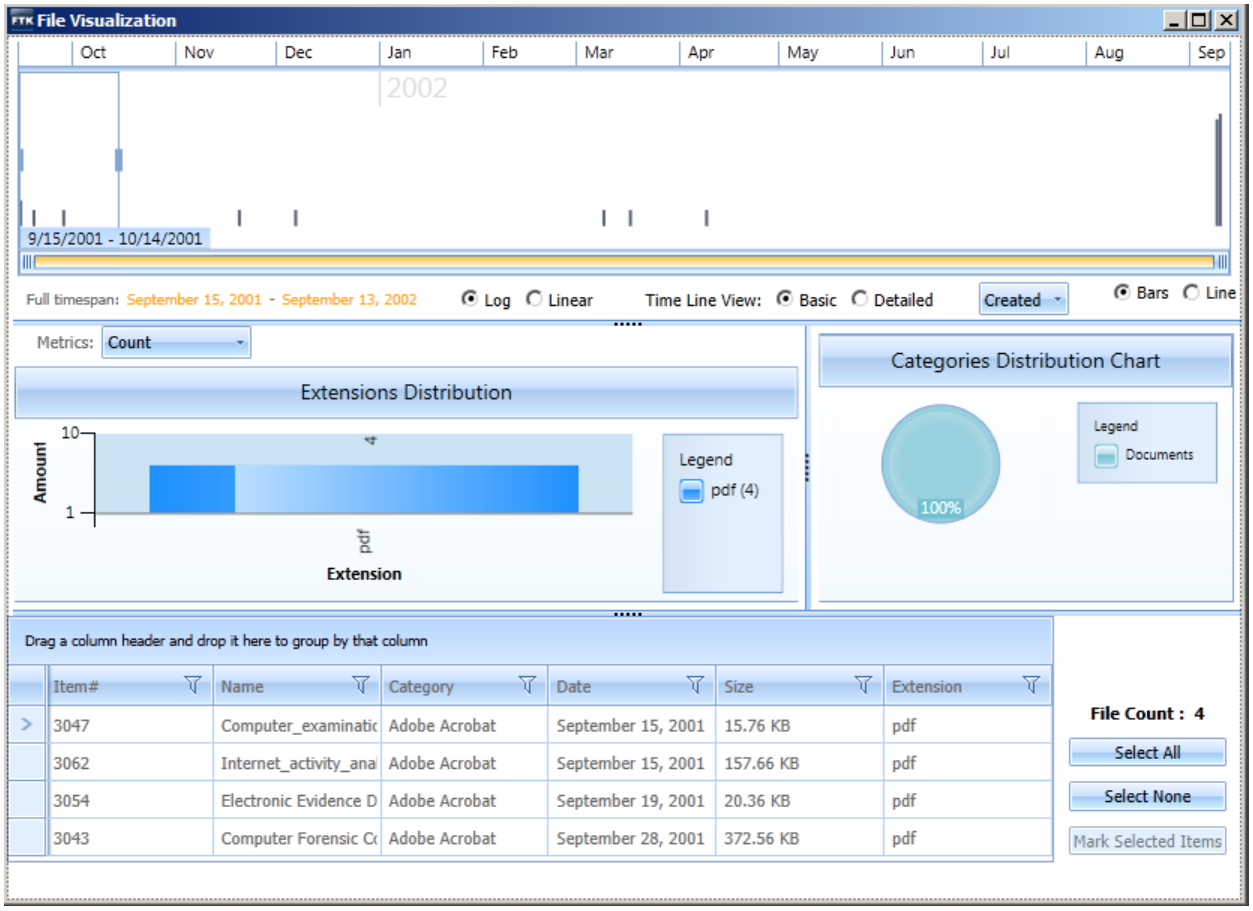
Important: The dashboard and data list displays information only for the data that exists in the base time line. If specified dates have no files, the dashboard displays the text “No Data Series.” To properly use Visualization, you must specify the base time line that you want to view data for.

About the Visualization page

The Visualization page includes three main components:

- Time line pane - Provides a time line pane with graphics representing the available data. This is the top part of the page.
- Dashboard - Provides graphical chart panes about the data. This is the middle part of the page.
- Data list pane- Provides a list of the data items. The is the lower part of the page.

You can resize each pane.



About Visualization Time Line Views

You can use one of the following two time line views:

- *Basic* - The basic view lets you specify a base time line that you want to view data for. For example, you can select a specific year or month, or you can specify a custom date range. Any data that falls in that date range will be represented in the charts and data list.

  See About the Base Time Line on page 431.

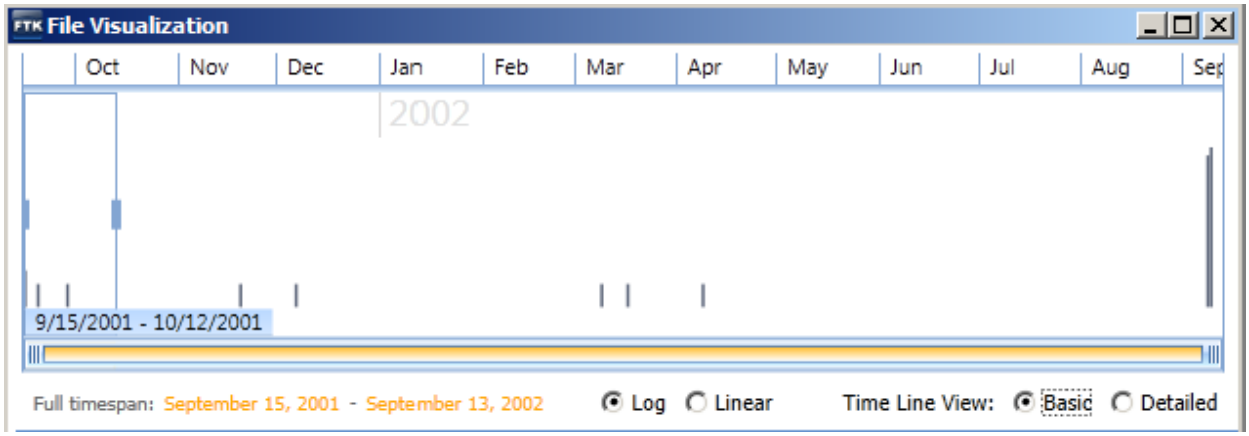
- *Detailed* - The detailed time line view shows a graphical representation of each file or email message. If you have a lot of data in a given date range, you can narrow your view to days, hours, minutes, and milliseconds.

  See About the Detailed Visualization Time Line on page 448.

About the Base Time Line

The top portion of the visualization page is the time line. The time line displays a graph with a representation of that data that is visualized. The data is displayed from the oldest date on the left to the most current date on the right.

The span of the time line is automatically configured based on the dates of the data that you specified for visualization. For example, if the data that you specified has creation dates that range from 8/15/2003 to 9/11/2003, it will build a time line with those dates as the start and end.



The vertical gray bars represent where the data files are on the time line. The gold text in the lower left corner of the time line details the full timespan.

In the *Basic* time line view, you configure the base time line. The base time line is the specific range of dates that you want to work with. This may be a smaller date range than the full timespan (dates in yellow).

The base time line is represented by the blue selection box with sliding vertical bars. You can modify the base time line to be any range within the full timespan.

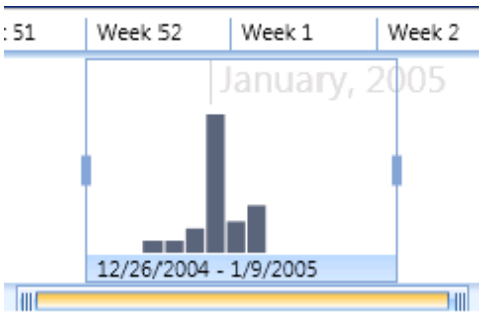
Important: The dashboard and data list displays information only for the data that exists in the base time line. If specified dates have no files, the dashboard displays the text “No Data Series.” To properly use visualization, you must specify the base time line that you want to view data for.

When you first launch visualization, a limited default base time line is specified, starting with the oldest data that is in the data set. For example, if you are viewing files, the default base time line is the first month starting with the creation date of the oldest file.

In the example in the graphic shown above, there are four files in the default base time line of one month and those four files are shown in the list and represented in the dashboard.

In the email visualization, the time line is displayed in weeks, with vertical gray bars representing the emails.

Time Line Selection Tools



Setting the Base Time Line

You adjust the range and the location of the base time line by adjusting the blue selection box. The information in the visualization dashboard and data list change when you adjust the selection box.

See About the Base Time Line on page 431.

To adjust the full timespan

1. Below the time line, you can zoom in on the view of the total timespan (yellow full timespan bar) by clicking and dragging the end of the bar.
2. You can also slide the yellow bar left or right to adjust the range.

To adjust the base time line

1. You change the base time line of the data set by adjusting the blue selection box.
2. You can do one of the following options:
   - Select a period that is on the top of the time line, for example, a specific month like June.
   - Drag the sliders of the blue selection box to make it bigger or smaller.
   - Drag the selection box to a different position.
   - Use the mouse scroll wheel to move the selection box left or right.

Changing the View of Visualization

You can change the way that visualization looks. You can modify the way that bar charts in visualization appear. You can also change the color scheme of the visualization windows.

Modifying the Bar Chart Displays

You can use the radio buttons below the time line to change the appearance of bar charts in visualization.

Log (default)	The *Log* (logarithmic) view makes visualization adjust the bars or lines to raise the low points and lower the highs so that both are easier to view on a chart. This view smooths the peaks and valleys in the chart.
Linear	The *Linear* view returns the view from *Log* to an unadjusted representation of the data. Changing from the *Log* view to the *Linear* view shows more of the variance and spikes in the data.
Bars (default)	The *Bars* option makes Visualization show evenly-spaced bars to represent the data.
Line	The *Line* view makes Visualization show the data as an unbroken line with peaks and valleys, representing increases and decreases in the amount of data over time.

Changing the Theme of Visualization

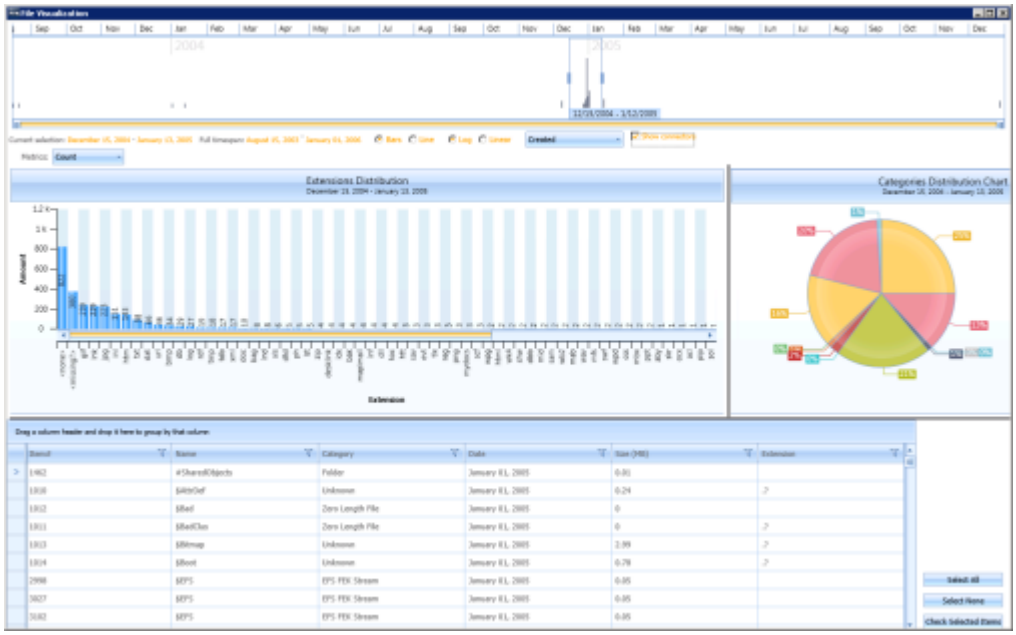
You can modify the appearance of the Visualization windows. You can choose from nine different color schemes.

To change the theme of Visualization

1. In the *Case Manager*, click **Tools > Preferences**.
2. In the *Preferences* dialog, under *Theme to use for Visualization*, choose from the following:
   - Office Blue (default)
   - Metro
   - Office Black
   - Office Silver
   - Vista
   - Windows 7
   - Summer
   - Expression Dark
   - Transparent

Visualizing File Data

The file data dashboard lets you view bar graphs, pie charts, and details about the files in the data set.



When visualizing files data, you can do the following:

- Configuring Visualization File Dates (page 435)
- Visualizing File Extension Distribution (page 436)
- Visualizing File Category Distribution (page 437)
- Using the File Data List (page 438)

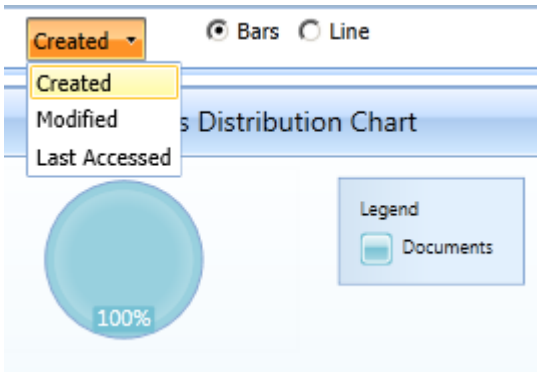
Configuring Visualization File Dates

When you view file data in the Visualization page, you can view data based on the following file data:

- Created date
- Modified date
- Last accessed date

If a file contains a Created date but not a Modified date, and you change the pane to display the file by Modified date, the file is no longer displayed in the visualization pane.

If a file's Created date, Modified date, or Last Accessed date is prior to the year 1985, visualization displays a dialog box. The dialog box asks you if you want to include the files with these dates in the visualization display. If you select the option to *Do not ask me again*, Visualization will remember your preference the next time the dates precede 1985.



Configuring the file date type

1. On the Visualization page, click the file date type drop-down menu.
2. By default, it displays the Created setting.
3. Select **Created**, **Modified**, or **Last Accessed**.

Visualizing File Extension Distribution

The extension distribution chart lets you view the data for the selected date range.

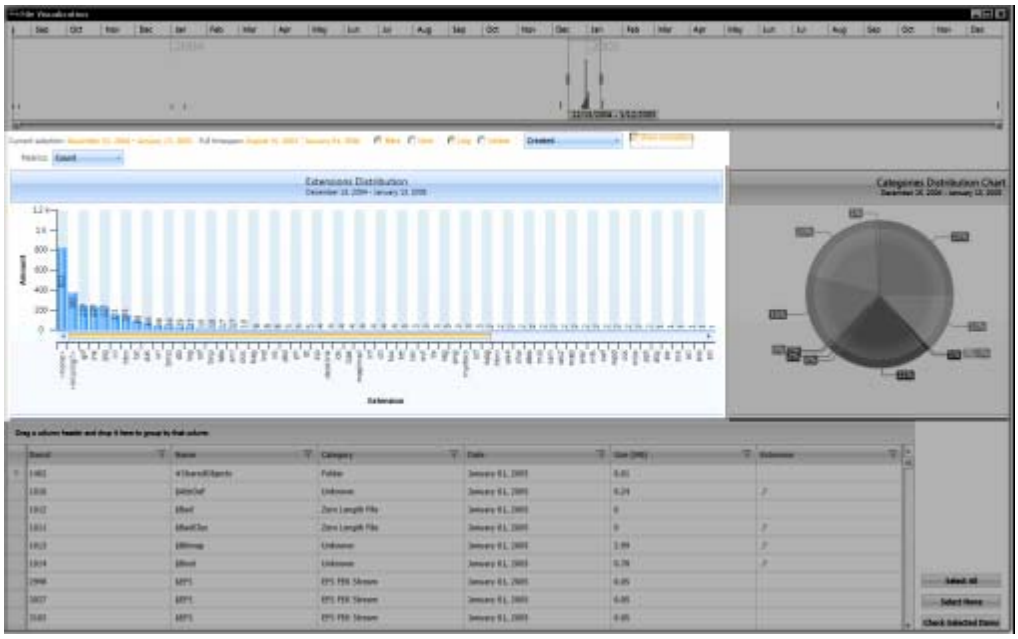
You can view selected data by the following ways:

- File extension counts
- File sizes

File counts and sizes are rounded to two decimal places. You can select a bar in the extension distribution chart to further refine the data that is displayed in the file data list.

You can select an extension in the legend to select or un-select extensions.

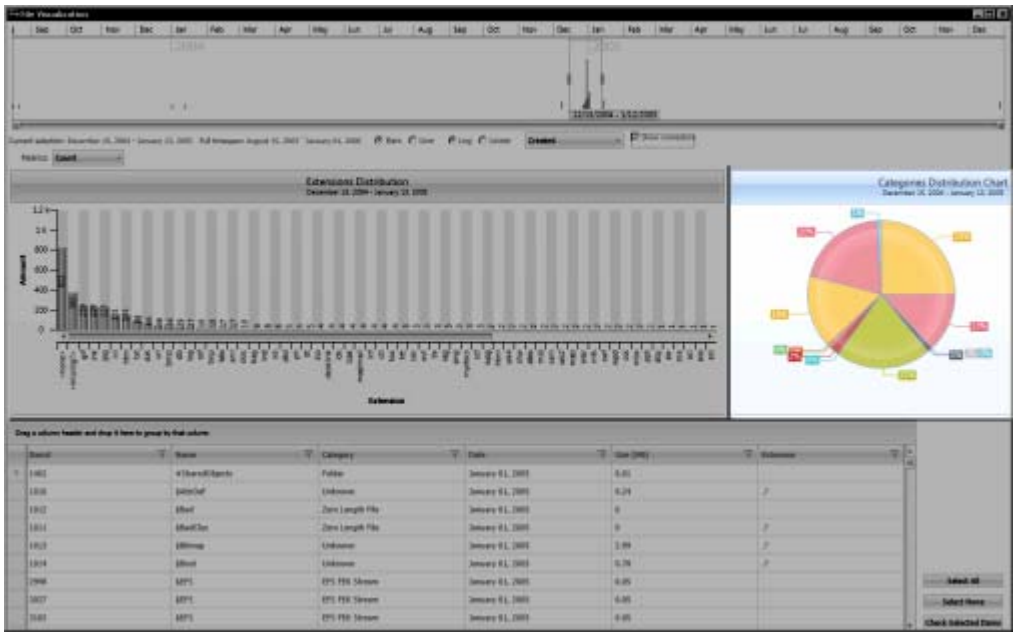
File Extension Distribution Pane



Visualizing File Category Distribution

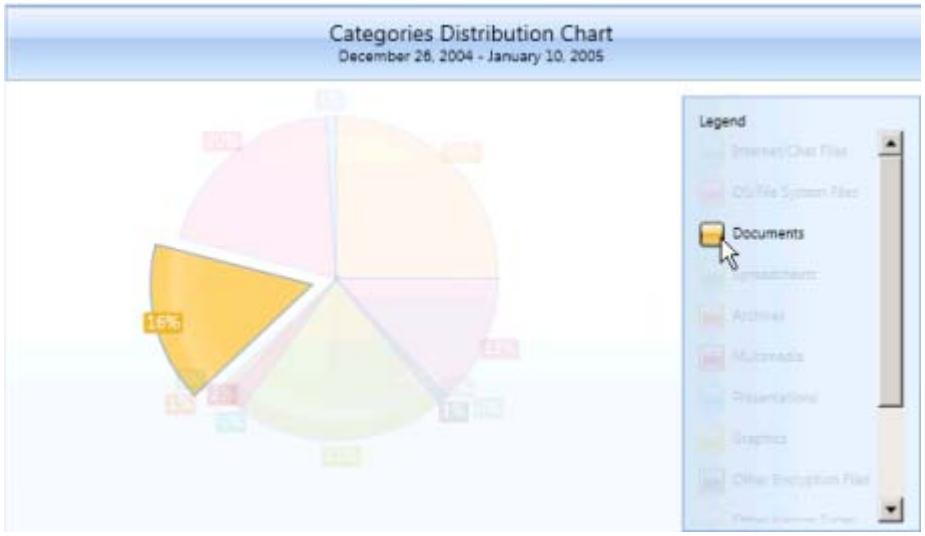
The category distribution chart displays a pie chart of the data set. It is organized according to the categories of the *Overview* tab and displays the percentages of each category in the data set. The percentages are displayed as the nearest whole number. For example: 10%. However, if a section in a category represents less than 1 whole percent, then the percentage is displayed to the hundredth percent. For example,56%.

Visualization Category Distribution Chart



If several categories are displayed very closely together, they may overlap and it can be difficult to read the percentages. You can click the **Show Connectors** option to expand the percentages further from the pie chart and include a connecting line to the pie section that correlates to the percentage.

You can select a category in the pie chart to further refine that data that is displayed in the file data list.

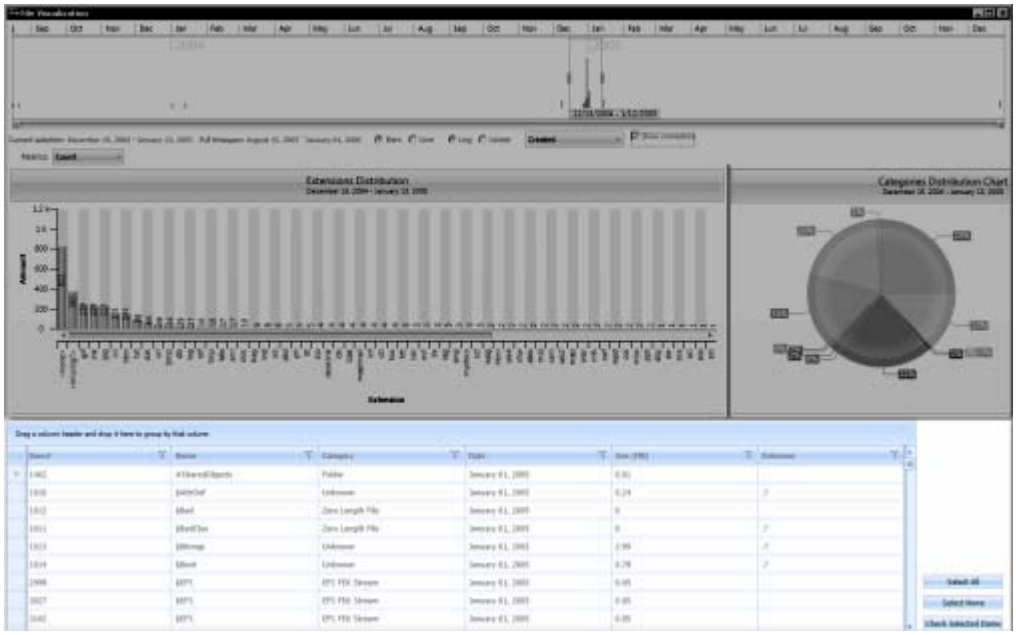


Using the File Data List

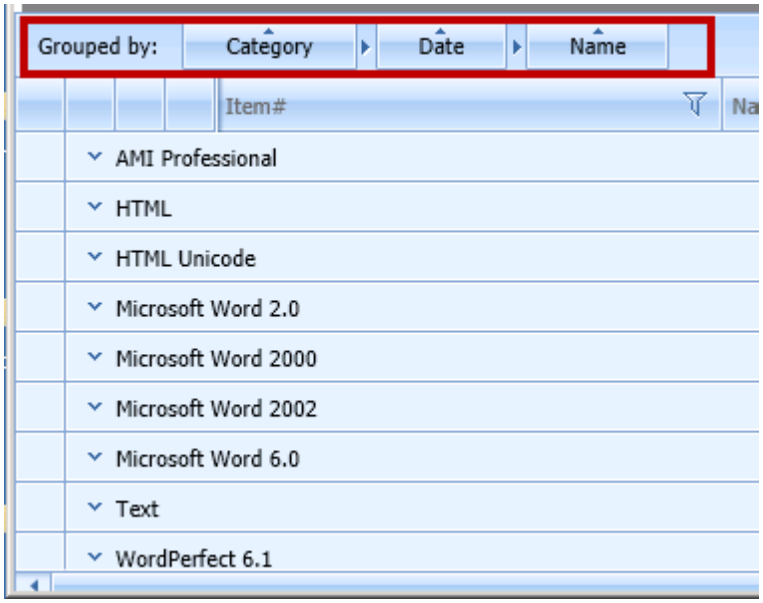
The file data list displays detail about the files in the data set. The pane is similar to the File List pane in the *Examiner* interface. The information that is displayed in the file data list is generated based on the data that you

refine through the use of the time line pane, the file extension distribution chart, and the categories distribution chart.

Visualization File Data List



Within the file data list you can sort, group, and sub-group, items according to columns including; ID, Name, Category, Date, and Size. To sort, drag and drop the desired column heading onto the blue bar. Any column heading that includes a filter icon can be used to sort the file list data set.

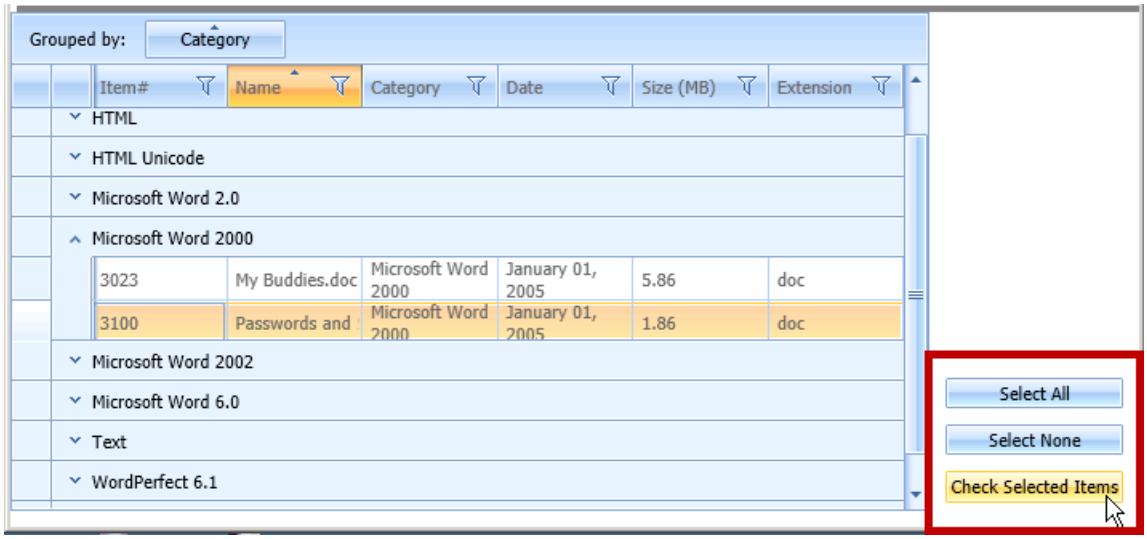


Important: If you want to filter for a specific date, include the day of and the day after. The filter uses midnight as the time frame. So if you only want files with a date of January 27, 2013, include January 27 and Jan 28. That will include files from midnight on the 27th to midnight on the 28th.

You can perform several actions on selecting the files and then clicking the **Mark Selected Items** button.

You can do the following:

- Label the item
- Create a bookmark from the item
- Clear a check mark if you have checked it.
- Check the item.

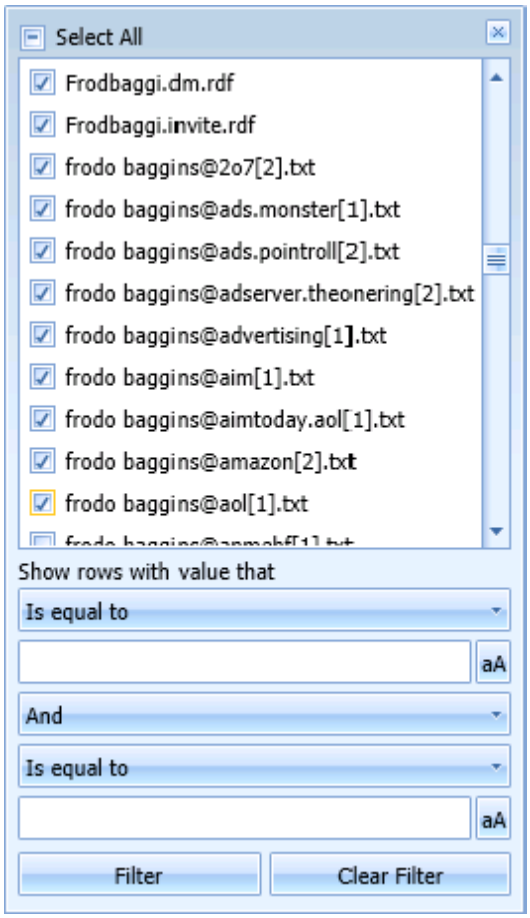


You can use the Filter icon on any of the column headings to create custom filters in the file details list.

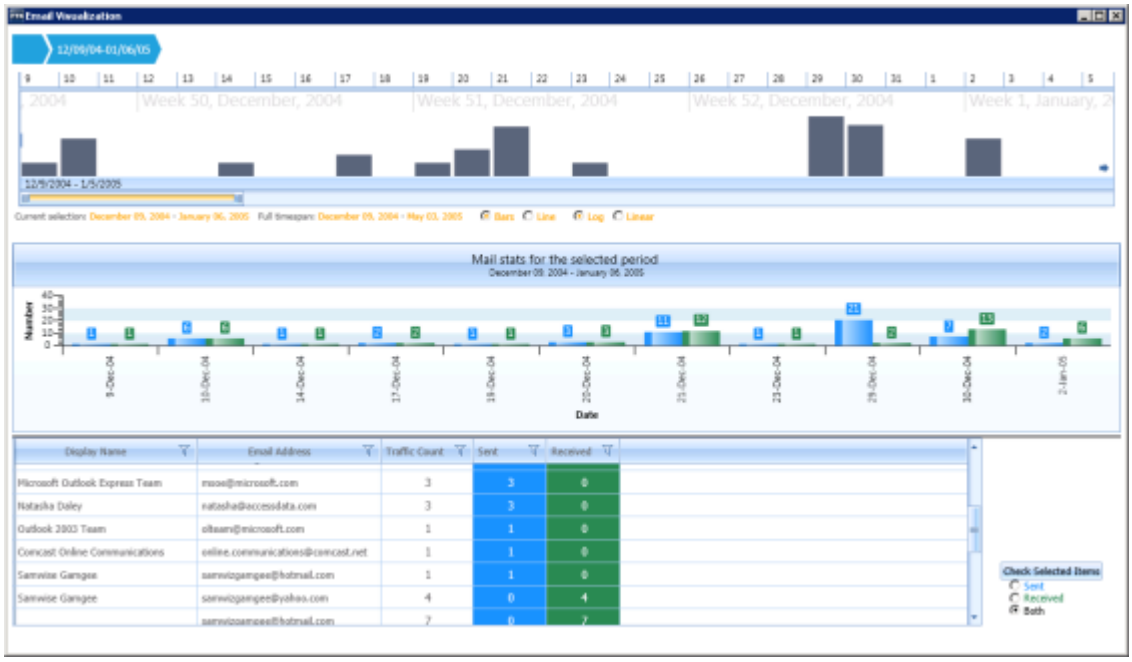
When you select the filter icon, a filter dialog is displayed that lets you select items that apply to the column where you add filtering expressions. There are many various was in which you can filter to refine the data that is displayed.

Note: You can filter and sort by file sizes such as bytes, KB, and MB. However, note that when you enter an operator to filter by size, you must enter the size according to its byte value. You cannot enter the value in KB or MB. For example, instead of entering 100 KB, you must enter 102400 for the filter to work properly.

File Data List Filtering Tool


Select All
Frodbaggi.dm.rdf
Frodbaggi.invite.rdf
frodo baggins@2o7[2].txt
frodo baggins@ads.monster[1].txt
frodo baggins@ads.pointroll[2].txt
frodo baggins@adserver.theonering[2].txt
frodo baggins@advertising[1].txt
frodo baggins@aim[1].txt
frodo baggins@aimtoday.aol[1].txt
frodo baggins@amazon[2].txt
frodo baggins@aol[1].txt
Show rows with value that
Is equal to
aA
And
Is equal to
aA
Filter
Clear Filter

Visualizing Email Data



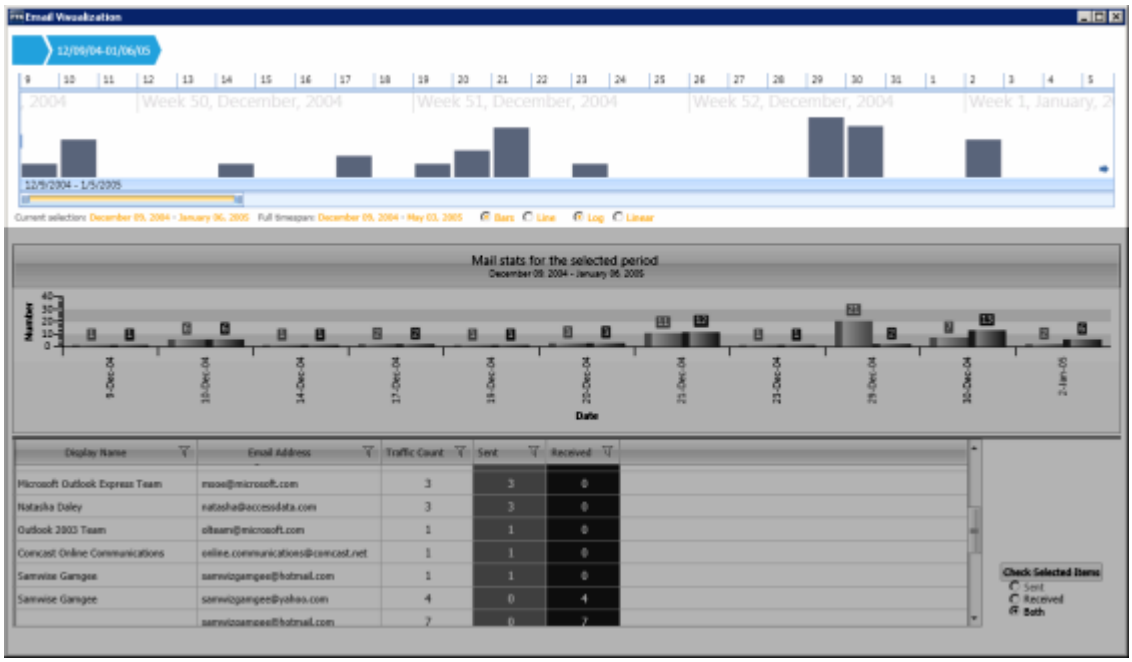
The email visualization dashboard consists of the following items:

- Email Time Line
  See Narrowing the Scope with the Email Time Line on page 442.
- Mail Statistics Graph
  See Viewing Mail Statistics on page 444.
- Email Details List
  See Using the Email Details List on page 444.
- Social Analyzer Chart
  See Using Visualization Social Analyzer on page 457.

Narrowing the Scope with the Email Time Line

The time line provides an aggregate view of email items sent and received in the data set. You can scale and refocus the scope of the time line to a specific data range. You can change the scope and scale of the data set by adjusting the gray slider tool. You can change the focus of the data set by adjusting the blue slider tool.

Visualization Email Date Pane

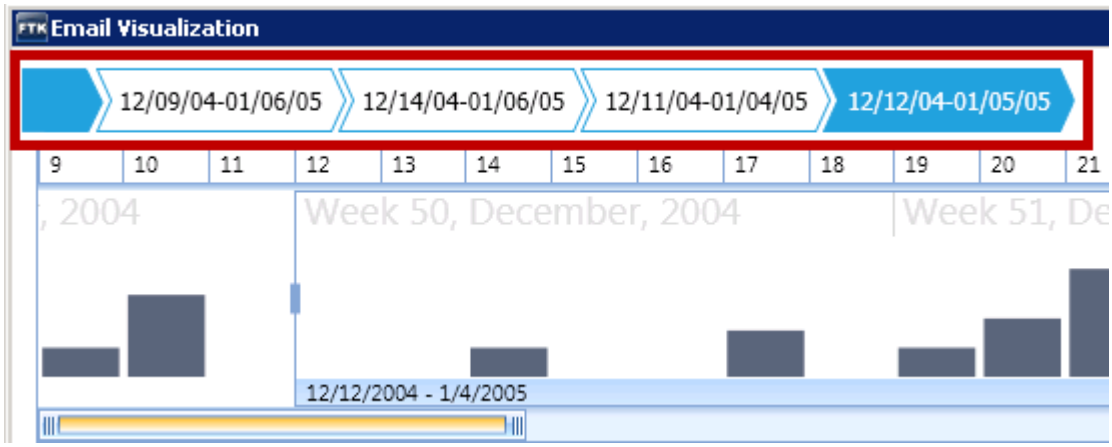


See also Setting the Base Time Line (page 433).

Using History Items in the Email Time Line

In the Email Visualization pane, when you alter the selection in the time line, a history item, also called a “bread crumb,” is added to the top of the time line. Each history item is labeled according to the date range that you have selected in the time line. You can use these history items to move forward or backward through different views that you have created.

Visualization History Items

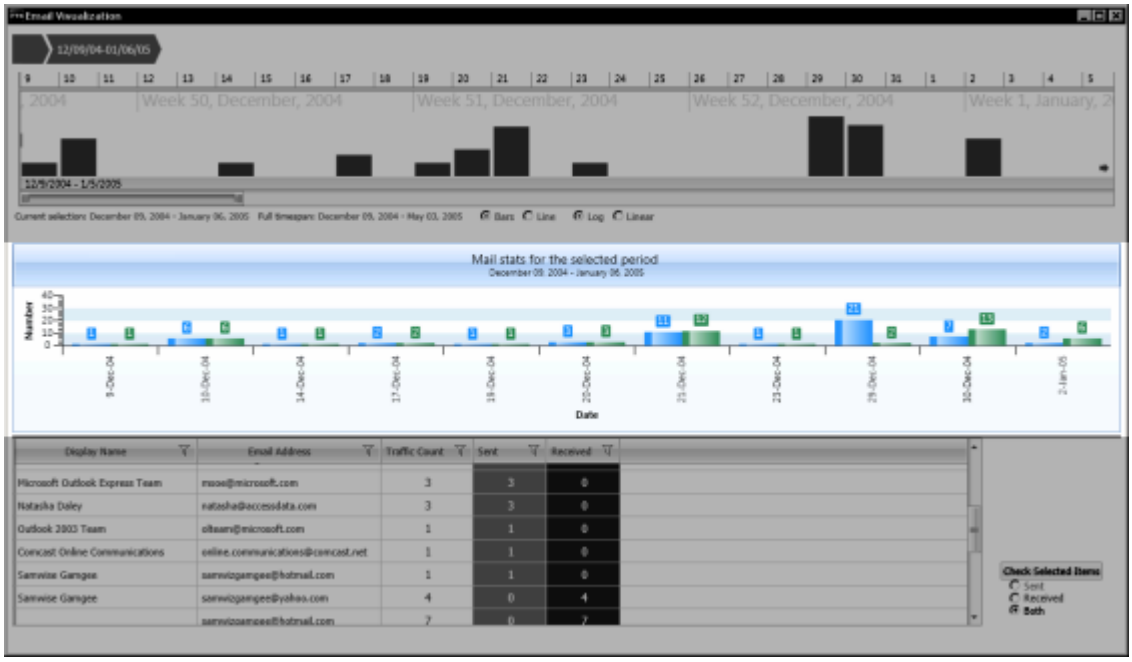


Viewing Mail Statistics

The mail statistics graph displays the sent and received mail statistics in a bar chart. The data contained within the date range, in the email time line, determines the data that is displayed in the mail statistics graph.

You can select a bar in the statistics graph to further refine the data that is displayed below in the Email details list.

Visualization Mail Statistics Chart

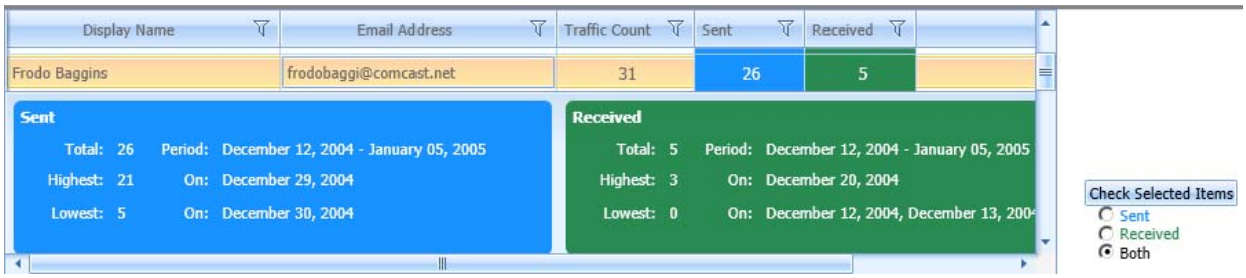


Using the Email Details List

The email details list displays custodian-level sent and received statistics for email items. The list contains a column for the custodian's name, a column for the custodian's sent mail, and a column for the custodian's received mail.

You can sort group and subgroup the emails according to the columns including: *Sender*, *Address*, *Traffic Count*, *Sent Mail*, and *Received Mail*. To group the list of emails, you can drag and drop the column headers onto the table heading of the details list. The list sorts first by the first columns that you drop, and then in the order of any preceding columns that you drop into the table heading.

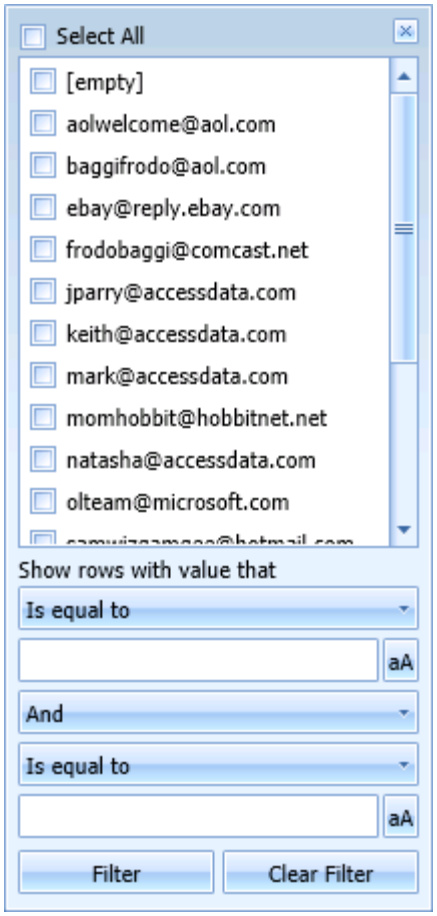
Visualization Email Details List



You can use the Filter icon on any of the column headings to create filters in the Email Details List.

When you select the Filter icon, a filter dialog is displayed that lets you select items that apply to the column and add filtering expressions.

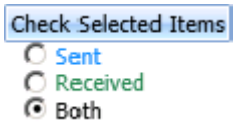
Email Details List Filtering Tool



In visualization, Email addresses that are similar but not exactly the same are displayed as two different addresses, even though they may be the same address. For example, the quotation marks for 'John Doe' and “John Doe” are not the same. These slight changes in text can happen from different email servers/software during email transit, and the program cannot discern duplicate email addresses.

If an email item is sent to multiple recipients, it is counted as a single item in the email details pane. In the Traffic Details chart, you can see when the same email was sent to multiple recipients. To view specific information about the recipients of that email item, you can click the **Traffic Details** button.

You can check specific emails in the examiner from the email details list by selecting the emails and then choosing one of the Check Selected Items options, *Sent, Received,* or *Both.*



When you expand a specific email item, you can run additional functionality. This functionality includes the Social Analyzer chart. The buttons to open the Social Analyzer chart are located on the right side of a custodian's email item in the list.

For more information see the following:

Using Visualization Social Analyzer (page 457)

Analyzing Email Domains in Visualization

Once you have you opened the Social Analyzer pane, you can isolate and examine individual email domains.

Note: Social Analyzer is very graphics-intensive. In order to avoid server issues, you should cull the data with facets and other filters to isolate the information that you want to examine before viewing it in Social Analyzer.

To analyze email domains in Visualization mode

1. Open **Social Analyzer**.
2. Click the domain bubbles to select the domain(s) that you want to view.
3. (optional) If you want to view the top ten domains in terms of received emails. click . Each time you click this icon, the next top ten bubbles will be selected, and so forth.
4. (optional) You can zoom in and zoom out of the Social Analyzer panel. If you hover over a domain bubble, the full display name and address, as well as the count, is displayed in the tool tip.
5. You can expand selected email domains and examine individual emails in a domain. See Analyzing Individual Emails in Visualization on page 446.

Analyzing Individual Emails in Visualization

You can expand email domains to display individual emails and the traffic between those emails.

To analyze individual emails within selected email domains

1. Open **Social Analyzer**.
2. Click the domain bubbles to select the domain(s) that you want to view.
3. (optional) If you want to view the top ten domains in terms of received emails. click . Each time you click this icon, the next top ten bubbles will be selected, and so forth.

4. (optional) You can zoom in and zoom out of the Social Analyzer panel. If you hover over a domain bubble, the full DisplayName and address, as well as the count, will be displayed in the tool tip.
5. Click to expand the domain names to display the individual emails.

Posting Email Results Back to the Examiner

After you have identified emails that are relevant to your investigation, you can post them back to the Examiner for further review. For example, you may drill down to an certain individual that had sent 25 emails to various domains. You can do the following:

- Add the 25 emails to a Label
- Add the 25 emails to a Bookmark
- Check the 25 emails in the F*ile List*
- Clear all other checked emails in the *File List* and check only these 25 emails.

To post email results

1. In the Social Analyzer, identify emails that you want to post.
2. Click **Post Results Back**.
3. Select the desired option.

About the Detailed Visualization Time Line

You can use the *Detailed* view of the visualization time line to get a more granular view of the files and emails in your data set. This helps you use the time line to identify the files and emails that are important in your investigation. The detailed view provides the following time bands that you can turn on or off to get a more or less granular view of the files:

- Years
- Months
- Days
- Hours
- Minutes
- Seconds
- Milliseconds

Different file types are represented by different colors to assist in identifying relevant files.

Using the Detailed Visualization Time Line

You can use the *Detailed* view of the time line to get a more granular view of the files and emails in your specified time line. You can change the *Time Line View* option to switch between the *Basic* view and the *Detailed* view.

Important: Before you launch the Detailed time line view, you must specify a base time line in the basic view that includes the data that you want to look at. Otherwise, you will only be able to see the files that are in the default base time line.

See About the Base Time Line on page 431.

To use the detailed visualization time line

1. Select a data set that you want to view.
2. Launch the visualization panel.
   See Launching Visualization on page 429.
3. Specify the base time line for the data that you want to view.
   See Setting the Base Time Line on page 433.
4. For the *Time Line View*, click **Detailed.**

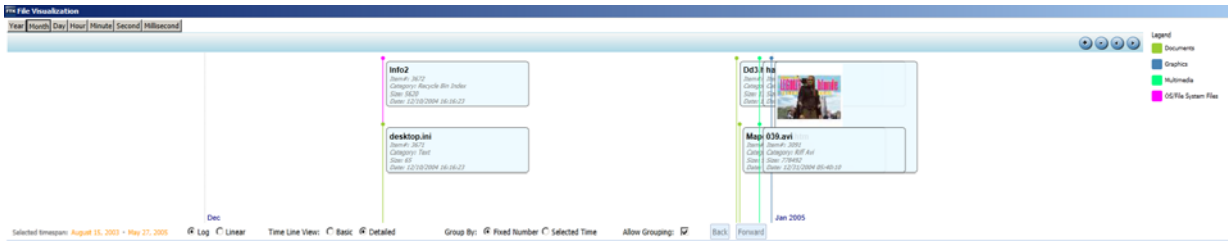
Understanding How Data is Represented in the Detailed Time Line

In the detailed view, each file, or group of files, is represented with a flag with a circle. Each flag displays the file's name, item number, category, size, and date. If you click a flag, the item it represents is selected in the file list pane at the bottom of the visualization interface.

The color of each flag and circle represents the type of data. For example, the color blue represents Graphics files. To the right of the time line, there is a *Legend* that displays what each color represents.

The span of the files depends on the base time line that you selected previously in the basic view.

See Setting the Base Time Line on page 433.



About Time Bands

If several items fall within a particular time frame, it can be difficult to see all of them. This is because their flags can overlap in the limited amount of interface space that is available.

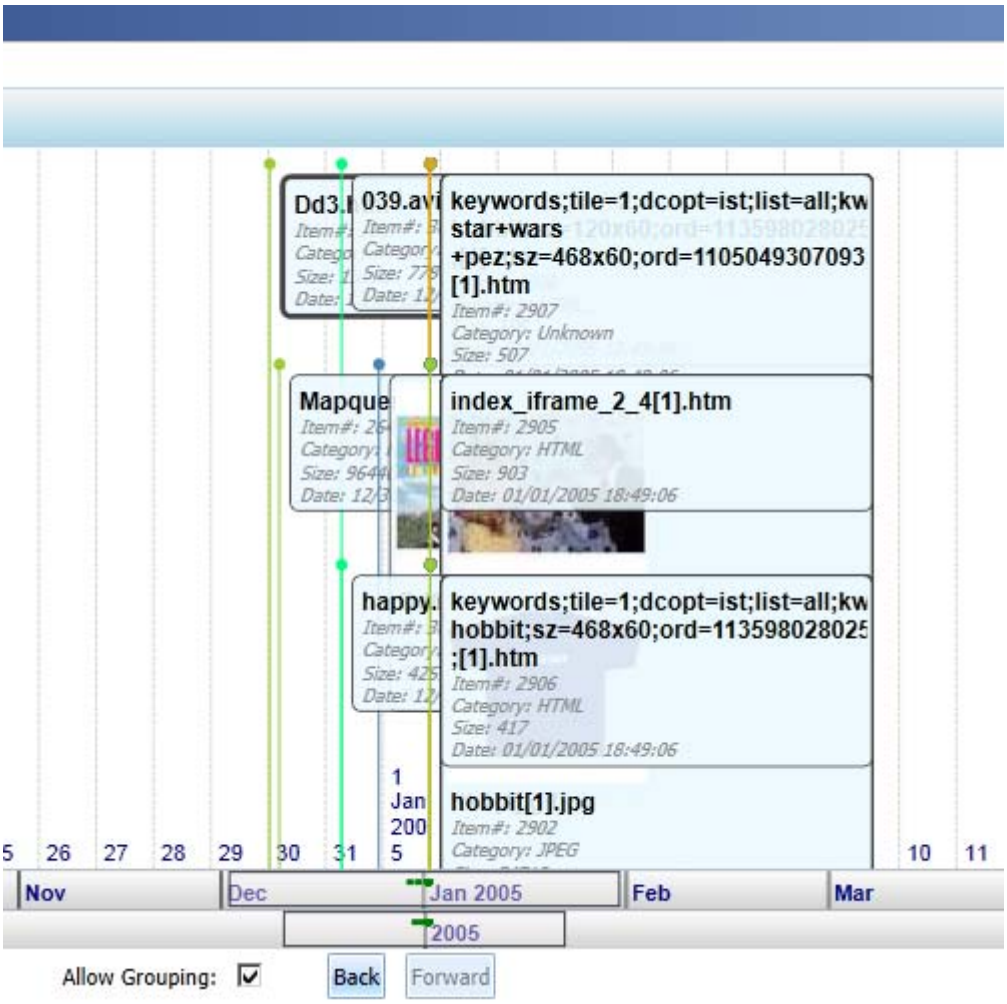
You can manipulate the time line by giving the time line a greater or less granular view by using different time bands. You can use one or more of the following time bands to change your view:

- Years
- Months
- Days
- Hours
- Minutes
- Seconds
- Milliseconds

When you first open visualization, it will determine which time bands to enable based on the date range of the base time line.

You can choose to display or hide a time band. The bands are displayed at the bottom of the time line. The more time bands that you turn on, the more granular the data becomes.

For example, suppose you turn on the Year, Month, and Day time bands.

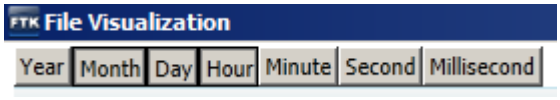


The Year time band is on the bottom, with the Month time band above that, and the Days time band (1-31) is above that. There are green dots in the bands. The green dots represent files or groups of files. Also in the example, there is a box in the center of the bands. That box is the view window. The view window is always in the center of the time line. You will only see the files that are in the view window. You can slide the time line to the left and right to place files into the view window.

If there are large clusters of files, you can turn on more time bands to get a more granular view of the files.

Modifying the Time Line Using Time Bands and Zoom

You can select different time bands to get a greater or less granular view of your data.



To change the time bands of the detailed time line

1. To display or hide a time band, in the top left corner, click a band to toggle it on or off.

   When a band is on, it is shadowed with a dark box.

   Be aware that when you change time bands, the focus box of that time band will be centered in the time line, and there may not be any files in the focus area. You will need to slide the time line to put the green dots back into the focus area.
2. Slide the time line to place the data in the view window.

   You can do one of the following options:

   - Click the right or left arrows in the upper-right corner.
   - Click the time line and drag it left or right.
   - Use the mouse scroll wheel to move it left or right.
3. You can also use the Zoom In and Zoom Out buttons (top-right corner) to modify the view.

   The zoom feature does not change the time bands or the selected date range. It simply displays more or less of the data.

Understanding How Grouping Works in the Detailed Visualization Time Line

If there are more than 500 items that all within a particular time period, the items are grouped together under a single grouped flag that represents all of the items. Grouping helps you to still use the detailed time line without having to view an overwhelming amount of data flags in a small amount of space.

You can have the data grouped by the following two methods:

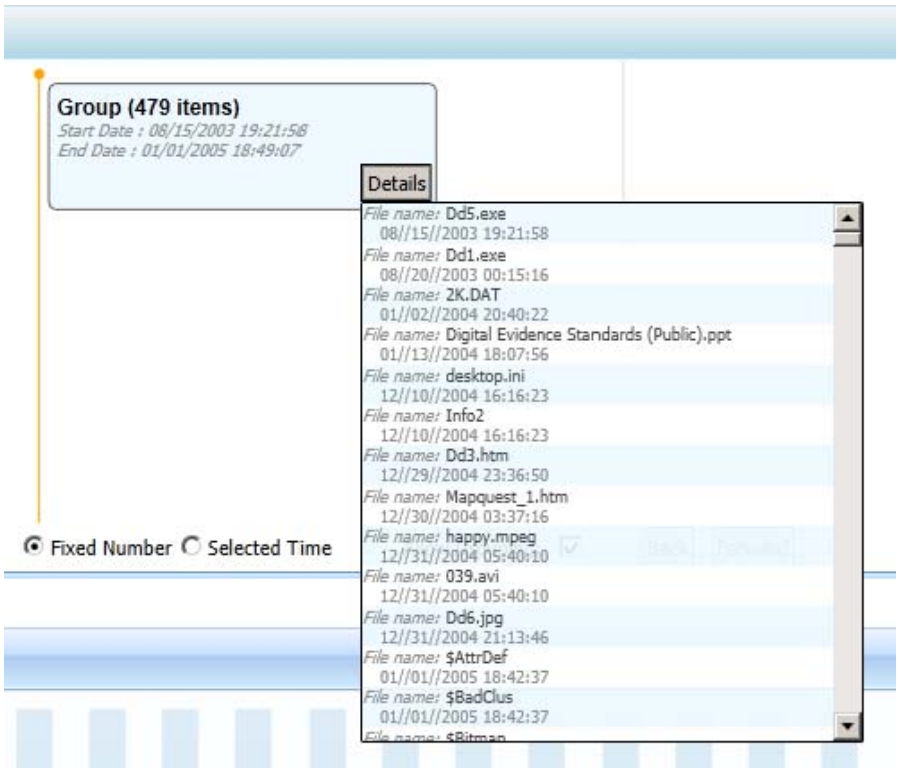
- Selected Time - (Default) Items are grouped by a specific time period, for example Days. For example, you could have 25 items on the 5th, 200 items on the 6th, and 1100 items on the 7th. There would be a single group for each day.
- Fixed Number - Items are grouped into by a maximum group size of 500. Using the previous example, if there were 1325 total items, they would displayed in three groups of 441 files.

The group flag includes a *Details* button. Click the Details button to display a list of all of the items that are grouped under that flag.

You can also click a group to get a more granular view of the files in the group. When you click a group additional time bands are enabled to give you a more detailed view.

Be aware that multiple flags may be staked vertically. You may need to make the time line pane taller by dragging the bottom border of the pane down.

Example of grouping


Group (479 items)
Start Date : 08/15/2003 19:21:58
End Date : 01/01/2005 18:49:07
Details
File name: Dd5.exe
08//15//2003 19:21:58
File name: Dd1.exe
08//20//2003 00:15:16
File name: 2K.DAT
01//02//2004 20:40:22
File name: Digital Evidence Standards (Public).ppt
01//13//2004 18:07:56
File name: desktop.ini
12//10//2004 16:16:23
File name: Info2
12//10//2004 16:16:23
File name: Dd3.htm
12//29//2004 23:36:50
File name: Mapquest_1.htm
12//30//2004 03:37:16
File name: happy.mpeg
12//31//2004 05:40:10
File name: 039.avi
12//31//2004 05:40:10
File name: Dd6.jpg
12//31//2004 21:13:46
File name: $AttrDef
01//01//2005 18:42:37
File name: $BadClus
01//01//2005 18:42:37
Fixed Number
Selected Time

Visualizing Internet Browser History Data

You can view internet browser history files in the detailed visualization timeline. You can view browser history from the following browsers:

- Internet Explorer
- Firefox
- Chrome
- Safari
- Opera

In order to view internet browsing history files in the detailed visualization timeline, you must first process the browser history files. By default, the option to process browser history files is disabled. You must enable the *Process Internet Browser History for Visualization* option in either the processing options or additional analysis options.

See Evidence Processing Options on page 90.

See Using Additional Analysis on page 141.

To view internet browser history files in the detailed visualization timeline

1. If you have browser history files, in the File List *Overview* tab, browse to **File Category** > **Internet Chat Files** > *browser name* > **History**.
2. Right-click one or more browser history files and select **Visualize Browser History...**

   View browser history files from only one manufacturer at a time.

   If the **Visualize Browser History...** option is grayed-out, then either the file has not been processed with the *Process Internet Browser History for Visualization* option enabled, or the file type is not supported.

   If it is a supported file, the detailed visualization timeline is opened.

   You may need to adjust the blue selection box to include the data that you want to see.

   For information on viewing the visualization timeline, see About the Visualization page (page 430).

Visualizing Other Data

You can process specific file types so that they can be viewed in the visualization timeline.

- EVTX files - See Viewing Data in Windows XML Event Log (EVTX) Files (page 310)
- IIS Log files - See Viewing IIS Log File Data (page 312)
- Registry data files - See Viewing Registry Timeline Data (page 314)
- CSV files that are in the Log2Timeline format - See Viewing Log2Timeline CSV File Data (page 316)

Chapter 32
Using Visualization Heatmap

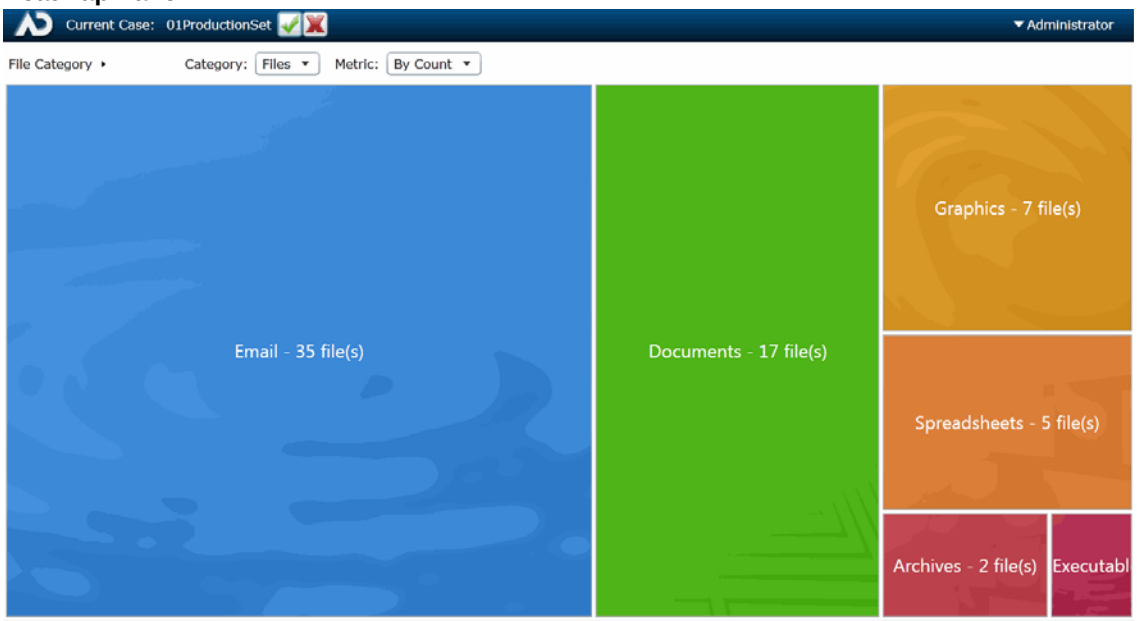
Heatmap allows you to view a visual representation of file categories and file volume within a project. Information displays in a grid comprised of squares of different colors and sizes. Each color represents a different file category, and the relative size of the square represents the file volume within the category. You can view each file category for more details about the files within that category (similar to a file tree) and navigate between file categories.

You can also switch between viewing the file volume by the physical size of each file and the file count. This allows you to see any discrepancies in the size of the files. For example, if someone were trying to hide a file by renaming the file extension, you could easily see the size discrepancy in the heatmap, and then investigate that particular file further.

To access Heatmap

1. In FTK, do the following:
   1a. Open the *Examiner*.
   1b. In the *File List* panel, click (Heatmap).
2. In Summation, do the following:
   2a. Click **Project Review**.
   2b. In the *Item List* panel, click **Options** > **Visualization** > **Heatmap**.

Heatmap Panel



Heatmap Options Panel

The following table defines the tasks from the **Heatmap** panel**.**

Heatmap Panel Options

Element	Description
	Cancels the heatmap filters and exits out of Visualization.
	Apply the visualization graph filters to the *Item List* grid. Once applied, only those items filtered with visualization appear in the *Item List* grid.
Options	

Category	• Files - Allows you to view files by the file category. You can view the files in each category:
	  ▪ By double-clicking that particular file category's square, or
	  ▪ By clicking the menu from the upper left side and choosing the file category that you want to view in the heatmap.
	• Folders - Allows you to view files by the folders contained within the project. You can view the files in each folder:
	  ▪ By double-clicking that particular folder's square.
	  ▪ By clicking the menu from the upper left side and choosing the folder that you want to view in the heatmap.
	• Extensions - Allows you to view files by the file extension.

Metric	• By Size - Allows you to view file types by size of the files. The larger the files, the larger the represented square in the heatmap. • By Count - Allows you to view file types by quantity. The more files of a particular type that are in the project, the larger the represented square in the heat map.

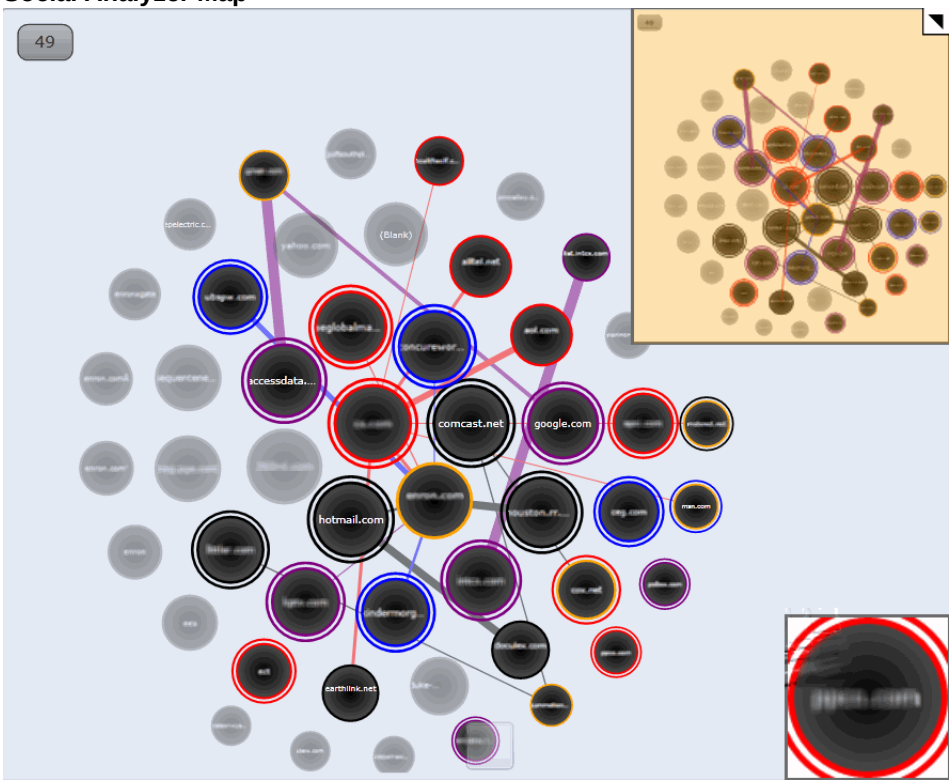
Chapter 33

Using Visualization Social Analyzer

About Social Analyzer

The Social Analyzer shows a visual representation of email volume contained in the data set. Social Analyzer will display all of the email domains in a project, as well as individual email addresses within the email domains.

Social Analyzer Map



The Social Analyzer map displays emails in the data set group by domain name. These domain names appear on the map in circles called “bubbles.” The larger the bubble, the more emails are contained within that domain. The bubbles in the map are arranged in a larger sphere according to how many emails were sent to that domain. The center bubble in the sphere will have the most emails sent from this domain, while domains radiating clockwise from the center will have fewer and fewer emails in their domain bubble. If you want to examine email domains with the most sent emails, concentrate on examining the bubbles in the center of the map.

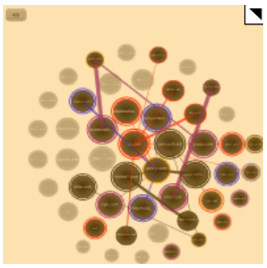
Email data in the Social Analyzer map can be examined on two different levels. On the first level, you can get an overall view of communications between domains. You can then select domains that you want to examine in a

more detailed view and expand those domains to view communications between specific email addresses from the domain. For example, if you search for high email traffic between two domains, you can see which two domains have the highest amount of traffic between them. Select the two domains, and expand them to view the email traffic between individual users from those two selected domains.

See Analyzing Email Domains in Visualization on page 461.

See Analyzing Individual Emails in Visualization on page 461.

Elements of the Social Analyzer Map

Element	Description
	This map presents the overall view of the social analyzer data. The orange rectangle indicates the area displayed in the main social analyzer map. Black dots in the overall view show domains that are either selected or communicating. You can either expand or collapse the overall view by clicking on the triangle in the upper right corner.
	When you select a domain bubble, it is surrounded by a colored double ring. The ring may be colored blue, black, purple, or red. The different colors allow you to distinguish between different selected domains, but they do not have any significant meaning.
	Domain bubbles that are not selected, but have sent emails to the selected domain bubble, are surrounded by a single colored ring that is the same color as the selected domain bubble. This allows you to easily tell which domains have been communicating with the selected domain bubble. Domain bubbles that do not connect to any selected domains are greyed out.
	Lines connect other domain bubbles to the selected domain bubble. These lines represent emails sent to the selected domain from other domains. The more emails that have been sent to the domain, the thicker the line between domain bubbles are. You can also see emails sent from the selected domain. Select **Show Reversed Connections** in the Social Analyzer panel to show visual representations of emails sent from the selected domain.
	A domain bubble with an orange ring indicates that a domain has been connected to from another domain multiple times. This allows you to pinpoint domains that have heavy communication between them.

Accessing Social Analyzer

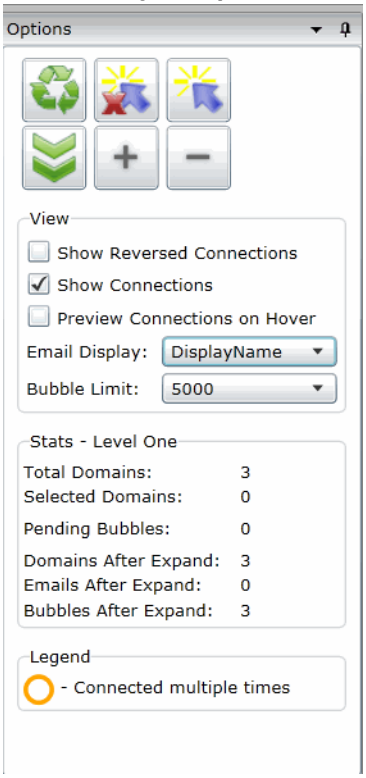
To navigate throughout the **Social Analyzer** pane, click and drag inside the pane. Hover over an email domain bubble to view the total number of emails that were sent from the domain.

Note: Expansion of large datasets may result in slow server speeds and slow rendering the Social Analyzer visualization data.

To access Social Analyzer

1. Click **Project Review**.
2. In the *Item List* panel, click **Options** > **Visualization** > **Social Analyzer**.

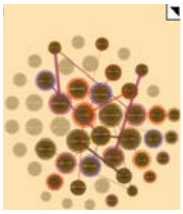
Social Analyzer Options Panel



Social Analyzer Options

The following table identifies the tasks that you can perform from the **Social Analyzer** panel**.**

Social Analyzer Options

Element	Description
Apply Visualization	Applies the visualization graph filters to the *Item List* grid. Once applied, only those items filtered with visualization will appear in the *Item List* grid.
Cancel Visualization	Cancels the visualization graph filters and exits out of Visualization.
Refresh	Refreshes the **Social Analyzer** pane.
Clear Selections	Clears the selected bubbles in the **Social Analyzer** pane.
Select Most Connected Items	Selects the ten bubbles that have been most connected to in the **Social Analyzer** pane. Each time you click this icon, the next top ten bubbles will be selected, and so forth.
Expand Selected Domains	Expands selected domains in the **Social Analyzer** pane. You can drill down to a second level to examine the email data. See Analyzing Individual Emails in Visualization on page 461.
Zoom In	Zooms into the **Social Analyzer** pane. If you are unable to view the social analyzer data, click **Zoom In** to locate the data. You can also zoom in by expanding the slider bar located at the bottom of the **Social Analyzer** pane, by using the **+** key on the keyboard, or by scrolling the mouse wheel up.
Zoom Out	Zooms out of the **Social Analyzer** pane. You can also zoom out by expanding the slider bar located at the bottom of the **Social Analyzer** pane, by using the **-** key on the keyboard, or by scrolling the mouse wheel down.
	Expands and collapses the overall map of the data set. Dots that appear in black in the overall map are domains/emails that are connected to the selected domain/email. The orange rectangle on the map shows where the expanded location is on the map.

Social Analyzer Options

Element	Description
View	• Show Reversed Connections - Select to show all reversed connections in the pane. Reversed connections are emails sent from a particular email or email domain. • Show Connections - Select to show the connections between domains in the pane. Connections are emails sent to a particular email or email domain. • Preview Connections on Hover - Select to view connections between domains when you hover over them. This option is not selected by default to speed rendering of the map. • Email Display - Display email domains either by the display name or address. • Bubble Limit - You can choose a display limit of either 2,500, 5,000, or 10,000 domains. Server issues may occur with larger display limits.
Stats	Displays the statistics of either the first or second level of the email domain data. You can view: • The total number of domains, emails, and bubbles in the pane. • The total number of selected domains, emails, and bubbles in the pane. • The total number of domains, emails, and bubbles that have been expanded. You can access the second level of data by clicking **Expand Selected Data**.

Analyzing Email Domains in Visualization

Once you have you opened the Social Analyzer pane, you can isolate and examine individual email domains.

Note: Social Analyzer is very graphics-intensive. In order to avoid server issues, you should cull the data with facets and other filters to isolate the information that you want to examine before viewing it in Social Analyzer.

To analyze email domains in Visualization mode

1. Click **Project Review**.
2. In the *Item List* panel, click **Options** > **Visualization** > **Social Analyzer**.
3. Click the domain bubbles to select the domain(s) that you want to view.
4. (optional) If you want to view the top ten domains in terms of received emails. click . Each time you click this icon, the next top ten bubbles will be selected, and so forth.
5. (optional) You can zoom in and zoom out of the Social Analyzer panel. If you hover over a domain bubble, the full display name and address, as well as the count, is displayed in the tool tip.
6. You can expand selected email domains and examine individual emails in a domain. See Analyzing Individual Emails in Visualization on page 461.

Analyzing Individual Emails in Visualization

You can expand email domains to display individual emails and the traffic between those emails.

To analyze individual emails within selected email domains

1. Click **Project Review**.
2. In the *Item List* panel, select **Options** > **Visualization** > **Social Analyzer**.
3. Click the domain bubbles to select the domain(s) that you want to view.
4. (optional) If you want to view the top ten domains in terms of received emails. click . Each time you click this icon, the next top ten bubbles will be selected, and so forth.
5. (optional) You can zoom in and zoom out of the Social Analyzer panel. If you hover over a domain bubble, the full DisplayName and address, as well as the count, will be displayed in the tool tip.
6. Click to expand the domain names to display the individual emails.

Chapter 34

Using Visualization Geolocation

About Geolocation Visualization

Geolocation allows you to view a map with real-world geographic location of evidence items that have geolocation information associated with them. This lets you understand where certain activities/actions took place.

See Using Visualization on page 148.

Geolocation supports the following data types:

- Photos with GPS information in the EXIF data. If you have photos in the evidence that have GPS data in the EXIF data, you can see where those photos were taken.
- IP location data after gathering Volatile data (Forensics products only). When using Forensic products and processing volatile/RAM data, you can see the lines of communication (both sent and received) between addresses, showing the location of all parties involved.

  Using Geolocation Visualization to View Security Data (page 472)

To use geolocation, you must enable the Geolocation processing option.

> **Note:** When using Forensic products, Geolocation IP address data may take up to eight minutes to generate, depending upon other jobs currently running in the application.

About Viewing Geolocation Data

When viewing Geolocation data, you can use the following components in Review:

- Maps

  When viewing geolocation data, you can use any of the following maps:

  - OpenStreetMaps
  - Offline Maps (See General Geolocation System Requirements (page 464) and Using Offline Maps (page 464))
- Geolocation Grid

  Below the map, you can view a grid that shows details about the items in the map.

  See Using the Geolocation Grid on page 469.

- Geolocation Data in columns in the *Item List*

  You can view geolocation data for files in the *Item List.*

  See Using Geolocation Columns in the Item List on page 470.
- Geolocation Facets

  There are specific facets for filtering on Geolocation data.

  See Using Geolocation Facets on page 471.

Important: When you launch the Geolocation view in Review, it will display all relevant files currently in the item list. You can cull the data using filters and other tools in the item list to limit the data that is displayed in Geolocation.

General Geolocation System Requirements

As a prerequisite, you must have the following:

- Access to a KFF Server.

  The KFF Server is configured by installing Elasticsearch. For Gelocation to work, no other KFF configuration (hashes and sets) is required.

  The KFF Server can be installed on the same computer as the AccessData software or on a separate computer.

  See *Getting Started with KFF* in the *Admin Guide*.
- Internet access to view web-based maps.

  By default, online maps are used to display map data for the Geolocation view.

  If you do not have internet access, you can download and use offline maps.

  See Using Offline Maps on page 464.
- For Forensic products (FTK, FTK Pro, Lab, and Enterprise):
  - The File Signature Analysis option selected when processing the evidence.
  - For using with IP data from volatile memory:
    - KFF Geolocation Data. This must be installed on the *KFF Server*.

Using Offline Maps

If you do not have internet access, you will not have access to the default online maps. You can download and use offline maps for Geolocation. You can use the offline maps with either eDiscovery, FTK, Lab, or Enterprise.

For more information, see:

https://support.accessdata.com/hc/en-us/articles/205757007-Geolocation-Maps-for-Offline-Use

Processing Geolocation Data

When you create a project, on the *Processing Options* tab, under *Miscellaneous Options*, you must select the **Geolocation** option.

Elasticsearch must be installed before processing the project. Otherwise, no Geolocation data is displayed.
See General Geolocation System Requirements on page 464.

Viewing Geolocation EXIF Data

When your evidence has photos with GPS information in the EXIF data, you can view photo locations.

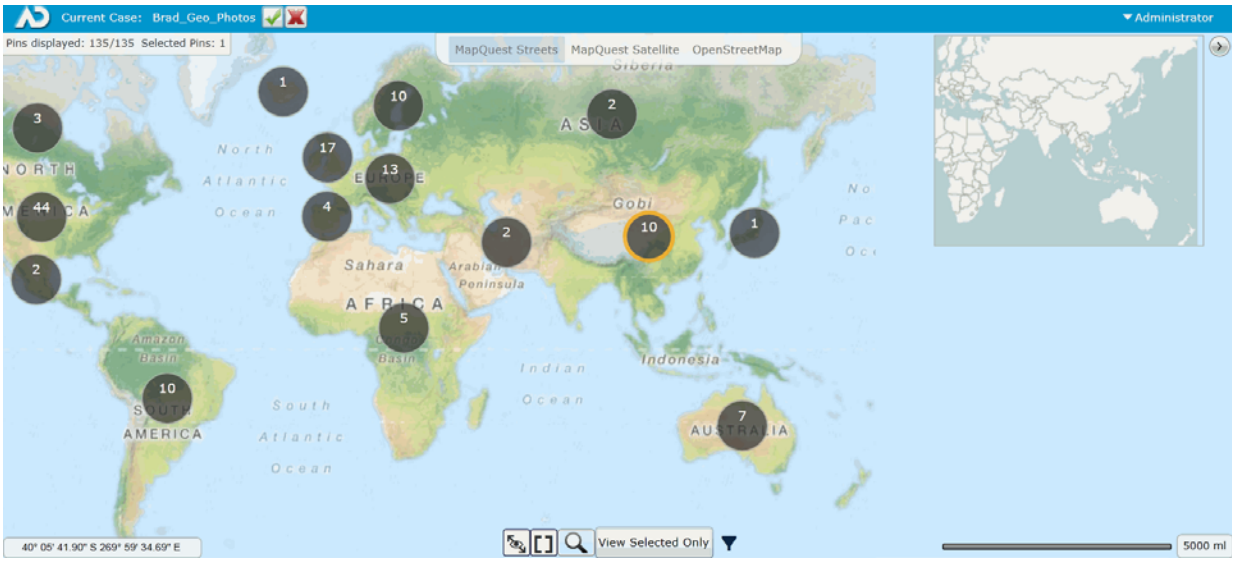
To view EXIF data in Forensic products (FTK, FTK Pro, Lab, and Enterprise):

1. In FTK, open the *Examiner*.
2. In the *File List* panel, click (Geolocation).
3. You can filter the items displayed and see item details.
   See Using the Geolocation Grid on page 469.

To view EXIF data in eDiscovery

1. Click **Project Review**.
2. In the *Item List* panel, click **Options** > **Visualization** > **Geolocation**.
3. You can filter the items displayed and see item details.
   See Using the Geolocation Grid on page 469.

Geolocation Panel - EXIF data



Using Geolocation Tools

The Geolocation Map Panel

Points of data in a particular area on the map are represented by large dots called clusters. The number on each cluster show how many points of data (known as pins) are represented by the cluster. Clicking a particular cluster on the map zooms in on a group of pins.

The general location of the clusters are determined by a central point on the map. The clusters radiate from this central point. When you zoom in and out of the map, your central point on the map moves as well, and clusters will shift position on the map. However, as you zoom into a cluster, the cluster rendered will more closely align itself with the location of the individual pins.

When viewing IP data, the connections between two pins display on the map as lines between clusters/pins. The width of the lines represent the amount of traffic between two IP address. The thicker the lines, the more traffic has occurred. Green lines represent traffic originating from the pin and red lines represent traffic entering the pin.

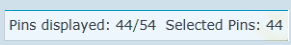
When you select a cluster and zoom in on a particular pin, you can select one or more pins. When a pin is selected, the outline and shadow of the selected pin turns orange. If you zoom out of the map, the cluster with one or more selected pins has an orange ring.

Hovering over the cluster displays the following icons:

- Selects all of the pins in a cluster.
- Clears all of the selected pins in a cluster.

The following table describes the Geolocation panel options.

Geolocation Panel

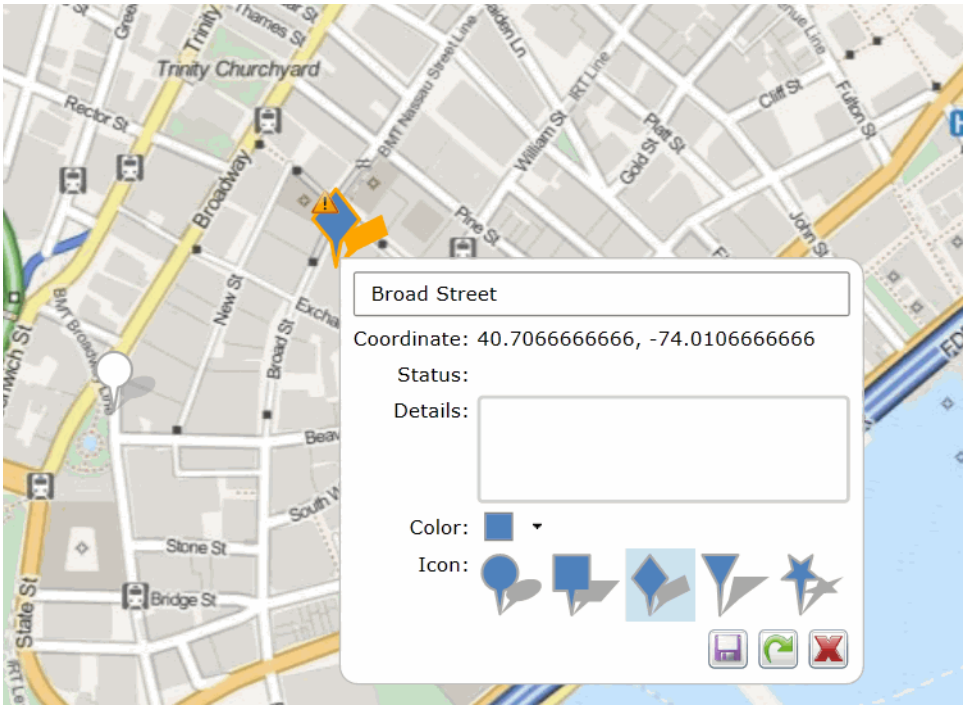
Element	Description
	After filtering data by selecting one or more pins, this applies the selected geolocations to the *Item List* grid. Once applied, only those geolocations filtered with visualization appear in the *Item List* grid. For network data, you will see any communication from those pins to any other location. This may include one or more items. If you enter the Geolocation view again, only those geolocation will be displayed in the map. To reset the items in the *Item List*, click the Project Explorer's *Reset* and *Apply* icons.
	Cancels the geolocation filters and exits out of Visualization.
Pins displayed	Shows the number of spins that are displayed and the number selected.
Clear	Clears and selected pins.
Options	
	Displays the number of pins selected in the map versus the number of pins available in the data.

Geolocation Panel

Element	Description
Map Tab	Choose which map to display in the *Geolocation* filter.
	Expands or collapses the overall view map.
29° 29' 15.39" N 118° 51' 23.18" W	Displays the latitude and longitude where the mouse pointer resides. To view the position of a particular pin, hover the mouse over the pin. To view the exact coordinates of the pin, select the pin and right-click.
	Turns the connections between the pins/clusters either on or off.
	Displays all of the pins on the map.
	Zooms in or out on the map. A slide bar displays, allowing you to control the zoom feature.
View All/View Selected	
Filter	Displays either EXIF data or network connection data. You can also view both types of data at the same time.

Right-clicking a pin displays more information about the pin.

Detail of Pin



In the pin dialog, you can:

- Add any notes
- View the exact coordinates and status of the pin

- View the IP Address of the pin

> **Note:** To save processing time and to ensure data accuracy, the host name does not populate in the Geolocation pin. However, the host name does populate in the Item List.

- Change the color and shape of the pin

If you make any changes to the pin, a warning icon displays that notifies you that changes were made to the pin and need to be saved. You can do the following in the pin dialog:

- Click to save the changes that you have made to the pin
- Click to reset the pin. If changes have been saved previously to the pin, this action resets the pin to the saved version
- Click to close the dialog

Using the Geolocation Grid

When you open Geolocation, you can view a grid that shows details of the items on the map.

The Geolocation Grid shows the following:

- **Exif:** This shows the following Exif data from photos
  - *Capture Data* column
  - *File Name* column
  - *File Size Coordinate* column

When you click an item in the grid, the map will be centered to reflect the location of the selected item.

You can minimize the grid so that the whole map is visible.

Filtering Items in the Geolocation Grid

When you first launch Geolocation, all of the items on the map are shown in the grid.

You can filter the contents of the grid in the following ways.

- In the map, if you select a pin, only that item is displayed. You can click (and select) multiple pins.
- In the map, if you right-click a cluster and click , that selects all of the pins in a cluster. This will filter the grid to those clustered pins. You can add multiple clusters to the grid.
- In the grid, the columns in the Geolocation Grid can be filtered to cull the items in the grid. For Network Communication data, the data in the bar chart is filtered as well when columns are filtered.

Using Geolocation Columns in the Item List

The data that the Geolocation filter uses to render the information is also available in columns in the *Item List*. You can find the following columns in the *Item List*, depending upon the data that has been collected. These columns can be sorted and filtered.

Data for geolocation columns require that the KFF Geolocation Data be installed.

See General Geolocation System Requirements on page 464.

Geolocation EXIF Data Columns

When your evidence has photos with GPS information in the EXIF data, you can view data using the following columns.

Geolocation Columns: EXIF data

Column	Display name	Description
Geotagged Area Code:	Area Code	Area code location of geotagged photo or object.
Geotagged City:	City	City location of geotagged photo or object.
Geotagged Country Code:	Country Code:	ISO country code location of geotagged photo or object, such as USA, FRA, MEX, HKG, and EST.
Geotagged Direction:	Direction	Direction geotagged photo or object.
Geotagged Latitude:	Latitude	Latitude of geotagged photo or object.
Geotagged Longitude:	Longitude	Longitude of geotagged photo or object.
Geotagged Postal Code:	Postal Code	Postal code of geotagged photo or object.
Geotagged Region:	Region	Regional or State location of geotagged photo or object, such as NY, DC, IL, FL, and UT.
Geotagged Source:	Source	Source used to resolve geotagged GPS location to locality information.

Using Geolocation Column Templates

When using AD Forensics products, you can use the following Column Templates to help you quickly display Geolocation-based columns in the File List:

- *Geolocation* - Displays all available Geolocation columns.
- *GeoEXIF* - Displays all columns that contain EXIF-related Geolocation data.
- *GeoIP* - Displays all columns that contain IP-related Geolocation data.

Using Geolocation Facets

When using eDiscovery, you can also use facets to cull data based on Geolocation data.

See Geolocation Facet Category on page 136.

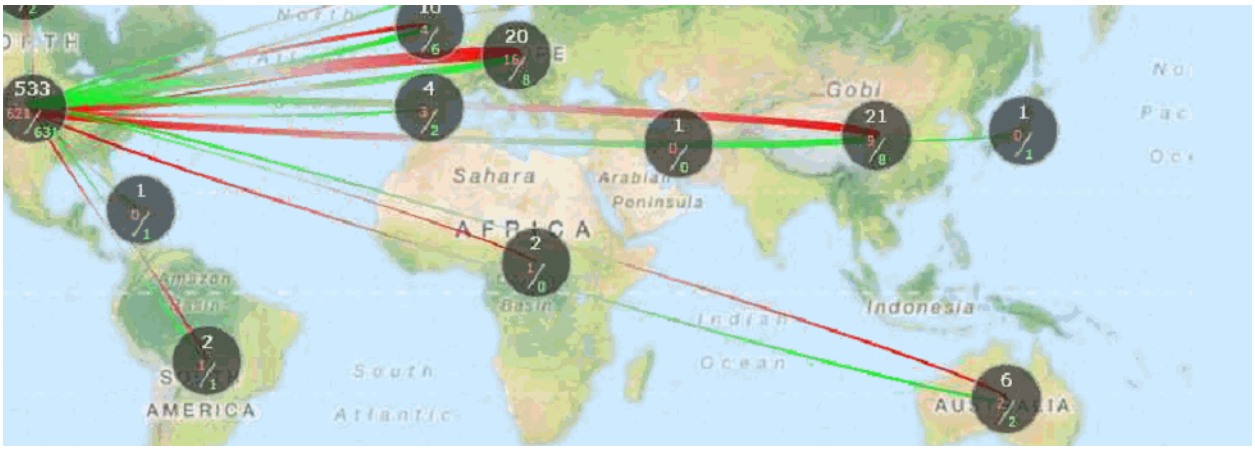
Using Geolocation Visualization to View Security Data

You can use geolocation to view IP location data to discover where in the world a computer is communicating. You can view IP locations data when using the following products:

- AD Forensics products, after gathering Volatile data

The Geolocation view will display lines that trace internet traffic sent and received between IP addresses, indicating the physical location of all parties involved. You can drill into geographic regions to see multiple evidence items. You can then select specific data to post back to the case, where they can view information in the examiner or include it in reports.

Geolocation Panel - IP Locations To view IP data in Geolocation viewer



Note: For data collected by Geolocation Visualization, the *To Domain Name*, *To ISP*, *To Netspeed*, and *To Organization* columns do not populate in the *Item Grid*. If you require this data, you need to purchase a MaxMind Premier database license.

Prerequisites for Using Geolocation Visualization to View Security Data

- For FTK or Enterprise:
  - For examining network acquisition and volatile data, enable the Geolocation option in the Web Config file. To enable this option, contact AccessData's support.
  - Also for examining network acquisition and volatile data, you need to generate a text file of your IP locations and place the text file in the GeoData directory. Configuring the Geolocation Location Configuration File (page 472)

Configuring the Geolocation Location Configuration File

When working with network acquisition and volatile data, some data may come from a private network where the physical location of the IP address is not known. For example, you may need to provide the location of your own network and any satellite offices that you interact with.

Normally you would start with block of IPs in your local network.

To set this information, you need to populate a configuration file for the KFF server.

The filename is **iplocations.txt.**

You can configure this file in one of two ways:

- Using the *Management* page > *System Configuration* > *Geolocation* page.
- Configuring the file manually

If you have already manually created this file, you will see the information in the configuration page interface.

Using the Geolocation Configuration Page

1. In the console, click *Management* > *System Configuration* > *Geolocation*
2. Click to add an item.
3. Fill in the location data. See Geolocation Configuration Page Options on page 473.
   See sample data below. You can get latitude longitude data for an area from Google maps.
   Any data you save here is saved in the configuration file.

Important: Any time you save new data, the KFF Service is automatically restarted. This can affect running KFF jobs.

Geolocation Configuration Page Options

The table below lists the various Geolocation Configuration Page options.

Geolocation Configuration Page Options

Option	Description
Ip Address	The IP address. The IP addresses must be written in CIDR format and need to be IPv4 addresses.
ID	
Country Code	The two letter country code for a country, such as HK for Hong Kong or US for the United States.
Country Code 3	The three letter country code for a country, such as RUS for Russia or DEU for Germany.
Country	The full country name, such as United States or Argentina.
Region	The state or province of the geolocation data, such as NY for New York or ON for Ontario.
City	The city of the geolocation data, such as Beijing or San Francisco.
Postal Code	The postal code or zip code of the geolocation data.
Latitude	The latitude of the geolocation data.
Longitude	The longitude of the geolocation data.
Metro Code	The metro code of the geolocation data.

Geolocation Configuration Page Options

Option	Description
Area Code	The area code of the geolocation data.
Continent Code	The continent code of the geolocation data. For example, NA for North America and AS for Asia.
Source	The source of the geolocation information. This field is optional.

Configuring the Location Configuration File Manually

You can manually create and edit the **iplocations.txt** text file for the KFF server. It has the following requirements:

- The text file needs to be saved with the filename **iplocations.txt**.
- The IP addresses must be written in CIDR format and need to be IPv4 addresses.
- Each comment line in the file must start with the character #. List only one address/network per line.
- The network line must contain the following information in the following order: address (in CIDR format), Id, CountryCode, CountryCode3, CountryName, Region, City, PostalCode, Latitude, Longitude, MetroCode, AreaCode, ContinentCode, Source.
- The **iplocations.txt** file must be placed in the **Geodata** folder of the **kffdata** folder on the server.

The following is an example of an **iplocations.txt** file:

```
#this file goes in the <kffdata>\GeoData directory
#address (in cidr
form),Id,CountryCode,CountryCode3,CountryName,Region,City,PostalCode,Latitude,Longitud
e,MetroCode,AreaCode,ContinentCode,Source
#192.168.0.0/24,1,,USA,United States,Utah,Taylorsville,84129,40.6677,-111.9388,,801,,
#10.10.200.252/30,1,,USA,United States,Utah,Orem,84042,40.2969,-111.6946,,801,NA,
#10.10.200.48/32,1,,USA,United States,Utah,Orem,84042,40.2969,-111.6946,,801,NA,
10.10.200.0/24,1,,USA,United States,Utah,Orem,84042,40.2969,-111.6946,,801,NA,
```

Viewing Geolocation IP Locations Data

To view IP location data in FTK

1. Open the *Examiner*.
2. Click the **Volatile** tab.
3. In the *Volatile* tab, click (Geolocation).
4. You can filter the items displayed and see item details.
   See Using the Geolocation Grid on page 469.

Using the Geolocation Network Information Grid

- When viewing network acquisition and volatile data connection information, you can now view a grid that displays the following information:
  - Process Start Time
  - Machine
  - User Name
  - Process Name
  - Path
  - Host Name
  - IP Address
  - Coordinates
  - Ports

You can show the communication between multiple pins.

Geolocation Filter

You can filter your Geolocation data with filters in the Facets Panel. The following filters are available under the Geolocation filter categories for security jobs that contain geolocation data.

Geolocation Filters in the Facets Panel

Geolocation Filters	Description
From Country Name	Filters evidence by the country from which the communication originated.
To Country Name	Filters evidence by the country to which the communication was sent.
From City Name	Filters evidence by the city from which the communication originated. Example: San Francisco, San Jose, Los Angeles.
To City Name	Filters evidence by the city that the communication to which was sent. Example: San Francisco, San Jose, Los Angeles
From Continent	Filters evidence by the continent from which the communication originated.
To Continent	Filters evidence by the continent to which the communication was sent.

Chapter 35
Customizing the Examiner Interface

This chapter includes the following topics

- About Customizing the Examiner User Interface (page 476)
- The Tab Layout Menu (page 477)
- Moving View Panels (page 478)
- Creating Custom Tabs (page 480)
- Managing Columns (page 481)
- Customizing File List Columns (page 481)
- Creating User-Defined Custom Columns for the File List view (page 482)
- Deleting Custom Columns (page 484)
- Navigating the Available Column Groups (page 484)

About Customizing the Examiner User Interface

You can use the View menu to control the pane views displayed in each tab. There are several tabs by default, but you can create an interface view that best suits your needs.

Add or remove panes from the current tab using the View menu. Click **View** and click the unchecked pane to add it to the current view, or click a checked item on the list to remove that pane from the current view.

To save the new arrangement

❖ Click **View > Tab Layout > Save**.

The View menu lets you do the following:

- Refresh the current view's data.
- View the Filter Bar
- Display the Time Zone for the evidence.
- Choose the display size for graphic thumbnails.
- Manage Tabs.
- Select Trees and viewing panes to include in various tabs.
- Open the Progress Window.

The Tab Layout Menu

Use the options in the Tab Layout menu to save changes to tabs, restore original settings, and lock settings to prevent changes.

The following table describes the options in the Tab Layout menu.

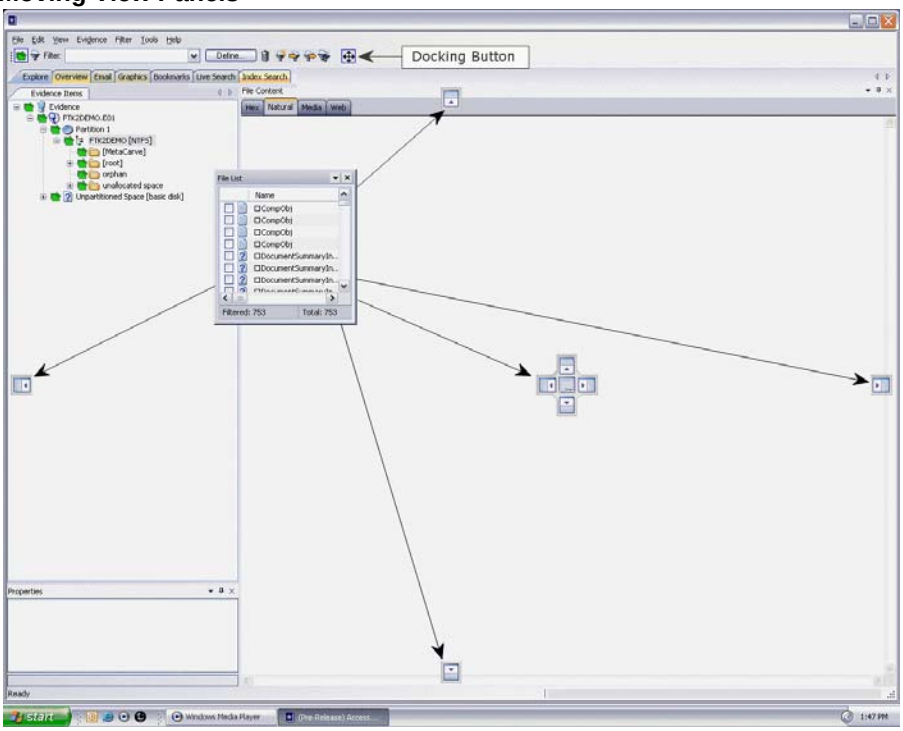
Tab Layout Menu Options

Option	Description
Save	Saves the changes made to the current tab.
Restore	Restores the *Examiner* window to the settings from the last saved layout. Custom settings can be restored.
Reset to Default	Sets the window to the setting that came with the program. Custom settings will be lost.
Remove	Removes the selected tab from the window.
Save All Layouts	Saves the changes made to all tabs.
Lock Panes	Locks the panes in place so that they cannot be moved until they are unlocked.
Add New Tab Layout	Adds a new tab to the window. The new tab will be like the one selected when this option is used. Customize the tab as needed and save it for future use.

Moving View Panels

Move view panes on the interface by placing the cursor on the title of the pane, clicking, dragging, and dropping the pane on the location desired. Holding down the mouse button undocks the pane. Use the guide icons to dock the pane in a pre-set location. The pane can be moved outside of the interface frame.

Moving View Panels



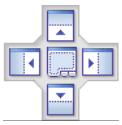
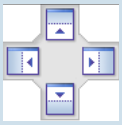
To place the view panel at a specific location on the application

1. Place the mouse (while dragging a view pane) onto a docking icon. The icon changes color.
2. Release the mouse button and the panel seats in its new position.
   The following table indicates the docking options available:

Docking Icons

Docking Icon	Description
	Docks the view panel to the top half of the tab.
	Docks the view panel to the right half of the tab.
	Docks the view panel to the left half of the tab.

Docking Icons (Continued)

Docking Icon	Description
	Docks the view panel to the bottom half of the tab.
	Docks the view panel to the top, right, left, bottom, or center of the pane. When docked to the center, the new pane overlaps the original pane, and both are indicated by tabs on the perimeter of the pane.
	Docks the view panel to the top, right, left, or bottom of the tree pane. The tree panes cannot be overlapped.
	Locks the panels in place, making them immovable. When the lock is applied, the blue box turns grey. This button is found on the toolbar.

Creating Custom Tabs

Create a custom tab to specialize an aspect of an investigation, add desired features, and apply filters as needed to accommodate conditions specific to a case.

To create a custom tab

1. Click on the tab that is most like the tab you want to create.
2. Click **View > Tab Layout > Add New Tab Layout**.
3. Enter a name for the new tab and click **OK**. The resulting tab is a copy of the tab you were on when you created the new one.
4. From the View menu, select the features you need in your new tab.

   Note: Features marked with diamonds are mutually exclusive; only one can exist on a tab at a time. Features with check marks can coexist in more than one instance on a tab.

5. Choose from the following:
   - Click *Save* to save this new tab's settings
   - Click *View* > *Tab Layout* > *Save*.
   - Click *View* > *Tab Layout* > *Save All* to save all changes and added features on all tabs.

To remove tabs

1. Highlight the tab to be removed
2. Click *View* > *Tab Layout* > *Remove*.

Managing Columns

Shared Columns use the same familiar windows and dialogs that Local Columns use.

To create a Shared Column Template

1. In *Case Manager*, click **Manage > Columns**.
   The *Manage Shared Column Settings* dialog opens.
2. Highlight a default *Column Template* to use as a basis for a *Custom Column Template*.
3. Click **New**.
4. Enter a new name in the *Column Template Name* field.
5. Select the Columns to add from the *Available Columns* pane, and click **Add >>** to move them to the *Selected Columns* pane.
6. Select from the *Selected Columns* pane and click **Remove** to clear an unwanted column from the *Selected Columns*.
7. When you have the new column template defined, click **OK**.

Customizing File List Columns

The Column Settings dialog box allows the modification or creation of new definitions for the file properties and related information that display in the File List, and in what order. Columns display specific information about, or properties of, the displayed files.

Column settings are also used to define which file information appears in case reports. Use custom column settings in defining reports to narrow the File List Properties information provided in the Bookmark and File List sections.

Additional states have been added to keep track of users' Label selections. For example, if the user has already checked a Label name, that filename and path will turn red, and it remains red as long as it remains different from the original status. Clicking it again will cycle it back to its original status and its color will return to black.

Note: Checking the Label name before choosing **Apply Labels To**, unchecks the Label name. Choose **Apply Labels To** first, then check or select the files to apply the Label to.

Column Settings can be customized and shared.

To define or customize Column Settings

1. From the *File List*, click **Column Settings** to open the *Manage Column Settings* dialog.
   From the *Manage Column Settings* dialog you can do any of the following tasks:

Button	Action
New	Create a new column template. This option opens a blank template you can use to create a new template from scratch.
Edit	Edit existing custom column templates. Use this option to make changes to an existing custom column template. You cannot edit default templates.

Button	Action
Copy Selected	Copy existing default or custom column templates. Start with the settings in an existing template to customize it to your exact needs without starting from scratch.
Delete	Delete existing custom column templates. You cannot delete default templates
Import	Import custom column templates XML files from other cases. Use Import to utilize a template from another source or that was created after you created your case.
Export	Export custom column templates to XML files for others to use. Export a custom column to use in another system.
Make Shared	Case Administrators can Share custom column templates to the database so they are available to all new cases. Once custom columns are Shared, the Application Administrator manages them. However, the original remains in the case so the Case Administrator has full control of it. Case Reviewers do not have sufficient permissions to create custom column templates.
Apply	Apply the selected column template

2. To define column settings using a new or copied template, click **New**, **Edit**, or **Copy Selected** to open the familiar Column Settings dialog.
3. In the Column Template Name field, type a name for the template.
4. In the Available Columns list, select a category from which you want to utilize a column heading.
   - You can add the entire contents of a category or expand the category to select individual headings.
   - You can move any item in the list up or down to position that column in the File List view. The top position is the first column from left to right.
5. When you are finished defining the column setting template, click **OK** to save the template and return to the Manage Column Settings dialog.
6. Highlight the template you just defined, and click **Apply** to apply those settings to the current File List view.

Creating User-Defined Custom Columns for the File List view

You can define your own custom columns for use in the File List view. You must first export a file list to a **TSV** or a **CSV** file from a case, then populate the spreadsheet with custom column names and your own data as it relates to items that are listed by the ObjectID. To add the resulting custom columns to the File List view, you simply import the **TSV** or **CSV** file that you created, add the custom columns to the template, and apply the template.

If you import a custom column sheet that contains a column that you do not want to import, but you do not want to delete the column, you can type IGNORE in the first row of the column.

Files saved as **TSV** or **CSV** are encoded UTF-8.

To define custom columns for the File List view

1. Open **CCExample.CSV** in a spreadsheet program. The default path to the file is **C:\Program Files\AccessData\Forensic Toolkit**[*version_number*]
   Use this example file to help you create your own custom columns.

2. In the *File List*, select the files that you want to add to your custom columns settings template.
3. From the *File List*, click **Export File List** .
4. In the *Save in* text box, browse to and select the destination folder for the exported file.
5. In the **File name** text box, type the first name of the file, but do not specify the extension.

> **Note:** You can overwrite user created column setting files by giving the column template the same name as an existing user created template. Be sure you provide a file name that is unique if you don't want to overwrite the original or existing column template file.

6. In the **Save As type** text box, click the drop-down and choose **CSV (Comma delimited) (*.**CSV**)**
7. In the **File List items to export** group box, click **All Highlighted**.
8. Click **Column Settings**.
9. In the Column Settings dialog box, ensure that **Item Number** is in the **Selected Columns** list. If desired, you can move it to the top of the list, or remove all other columns headings that are listed in the **Selected Columns** list.
10. Click **OK**.
11. In the *Choose Columns* drop-down, select the Column Setting you just created or modified.
12. Click **Save**.
13. Open the **CSV** file that you just created with the Export File List.
14. Copy the item numbers in the Item Number column.
15. In the opened **CCexample.CSV** file, paste the item numbers in the OBJECTID column.
16. Edit the column headings the way you want them.

    For example, the spreadsheet column, "MyCustomInt:INT" displays as the column heading "MyCustomInt" in the File List view.

    - Edit "MyCustomInt" to be whatever you want:
    - The INT portion allows integer values in the column
    - MyCustomBool:BOOL column allows true or false values
    - CustomStr:STRING heading allows text values.
17. Save the **CCExample.CSV** file with a new name, and in a place where you have rights to save and access the file as needed.
18. Close the **FileList.CSV** (or whatever name you gave the Export File List file.
19. On the Evidence menu, click **Import Custom Column File**.
20. Navigate to the **CSV** file that you just saved, then click **Open**.
21. In the "Custom column data imported" dialog box, click **OK**.
22. On the **Manage** menu, click **Column > Manage Columns**, or click Column Settings on the File List toolbar.
23. Choose a column template to copy, or create a new one.
24. Add the custom column headings to a new or existing template.
25. In the Column Settings dialog box, click **OK**.
26. In the Manage Column Settings dialog box, select the template that contains the custom headings, and then click **Apply**.

Deleting Custom Columns

You can remove and delete custom columns that you have added to any column templates. You can delete custom columns even if the File List view is turned off.

Note: The data is not deleted; only the custom columns that allowed you to see that specific data are deleted.

To delete custom column data

1. On the Evidence menu, click **Delete Custom Column Data**.
2. Click **Yes** to confirm the deletion.

Navigating the Available Column Groups

The Column Settings dialog box groups column settings according to the following:

Available Column Groups	
• Common Features	• Custom Columns (When a custom column template has been created or imported.)
• Disk Image Features	• Email Features
• Entropy Stats	• File Status Features
• File System Features	• Mobile Phones (When an MPE AD1 or other cell phone image has been processed.)
• ZIP-specific Features	• Office-specific Features
• Cerberus Static Analysis Features	• Microsoft IIS Internet Server
• Log2t	• Internet Data
• Geolocation	• All Features

Within each grouping, you can choose from a list of various column headings that you want to add. You can also delete selected columns or arrange them in the order you want them to appear in the File List view.

To view the name, short name, and description of each available column

1. On the **Manage** menu, click **Columns > Managed Shared Columns**.
2. Do one of the following:
   - Select a category.
   - Open a category and select an individual column setting name.
3. Do either of the following:
   - Click **Add >>** to move your selection to the Selected Columns list.
   - Double-click your selection to add it to the Selected Columns list.
4. Do either of the following.
   - Use standard Windows column sizing methods to resize the column margins, thereby allowing you to read each description.
   - Click anywhere in the Select Columns list box, and then hover over a column description to see the entire description.
5. Click **OK**.

Note: The following information may be useful when navigating or viewing Available Columns and Groups.

- When you view data in the File List view, use the type-down control feature to locate the information you are looking for. Sort on the Filename column, then select the first item in the list.

  Type the first letter of the filename you are searching for. As you continue to type, next filename that matches the letters you have typed will be highlighted in the list.

  If at some point you see the file you are looking for displayed in the list, simply click on it. You may type the entire file name for the exact name to be fully highlighted in the list.

- A new column has been added, “Included by Filters” within the All Features group. This column tells you which filter caused a file to display in the File List pane. The Included by Filters column is not sortable.

- In the past, the “Processed” column was able to display only two states, Yes, and No. It has been changed to display different states, such as the following:

  P = Default (may be a null value)

  C = Complete

  Note: *M* = User’s manually carved items

Chapter 36
Working with Evidence Reports

You can create a case report about the relevant information of a case any time during or after the investigation and analysis of a case. Reports can be generated in different formats, including HTML and PDF. The PDF report is designed specifically for printing hard copies with preserved formatting and correct organization. The HTML report is better for electronic distribution.

This chapter includes the following topics

- Creating a Case Report (page 487)
- Adding Case Information to a Report (page 488)
- Adding Bookmarks to a Report (page 489)
- Adding Graphics Thumbnails and Files to a Report (page 491)
- Adding a File Path List to a Report (page 493)
- Adding a File Properties List to a Report (page 494)
- Adding Registry Selections to a Report (page 495)
- Adding Screen Captures from Examiner (page 496)
- Selecting the Report Output Options (page 497)
- Creating a Load File (page 498)
- Viewing and Distributing a Report (page 501)
- Modifying a Report (page 502)
- Exporting and Importing Report Settings (page 502)
- Writing a Report to CD or DVD (page 503)

Creating a Case Report

You can use the *Report Wizard* to create a report. The the settings that you specify in the *Report Wizard* are persistent, and remain until they are changed by the user. You do not need to click **OK** until all the report creation information is entered or selected. If you inadvertently close the Report Wizard, you can re-open it by clicking *File* > *Report*.

To Create a Case Report

1. In the *Examiner*, click **File > Report** to run the *Report Wizard*.
2. Define your requirements for the following:

Option	Description
Case Information	See Adding Case Information to a Report (page 488)
Bookmarks	See Adding Bookmarks to a Report (page 489)
Graphics	See Adding Graphics Thumbnails and Files to a Report (page 491)
Videos	See Adding a Video to a Report (page 492)
File Path List	See Adding a File Path List to a Report (page 493)
File Properties ListSee	See Adding a File Properties List to a Report (page 494)
Registry Selections	See Adding Registry Selections to a Report (page 495)

3. When you have completed defining the report, click **OK** to open the *Report Output* options dialog. See Selecting the Report Output Options (page 497)

Adding Case Information to a Report

The *Case Information* dialog lets you add basic case information to a report, such as the investigator and the organization that analyzed the case.

For information about other items you can define for a report, See Creating a Case Report (page 487).

To Add Case Information to a Report

1. In the *Examiner*, click **File > Report**.
2. In the left pane, under *Report Outline*, highlight **Case Information** to display the *Case Information* options in the right pane.

   You can select the **Case Information** check box to include a case information section in the report. You can deselect the **Case Information** check box to exclude a case information section from the report.
3. In the *Default Entries* pane, deselect any entries that you do not want to include in the report.

   If you inadvertently remove a default entry that you require, close and reopen the case to have the default entries displayed again.
4. Double-click the **Value** field to enter information.
5. Add and remove entries with the **Add** and **Remove** buttons under the *Default Entries* section.
6. Provide a label (Name) and a value (Information) for the included entries.
7. (Optional) Select the **Include File Extensions** option to include a file extensions list and count in the File Overview portion of the report.

   The list of file extensions appears in the report under *Case Information*, after *File Items* and *File Category*, and before *File Status*. The *File Extensions List* can be very long and may span many pages. If you intend to print the report, this may not be desirable.

Adding Bookmarks to a Report

The *Bookmarks* dialog lets you create a section in the report that lists the bookmarks that were created during the case investigation. Each bookmark can have a unique sorting option and a unique column setting.

For information about other items you can define for a report, See Creating a Case Report (page 487).

To add Bookmarks to a Report

1. In the *Examiner*, click **File > Report**.
2. In the left pane, under *Report Outline*, highlight **Bookmarks** to display the *Bookmarks* options in the right pane.

   You can select the **Bookmarks** check box to include bookmarks in the report. You can deselect the **Bookmarks** check box to exclude bookmarks from the report.
3. In the right pane, click **Filter** to open the filters list.
4. Select one the filters from the list. The empty line at the top of the list lets you apply no filter to the bookmarks.
5. Select the options to indicate which bookmarks you want to include. Choose **Shared** and/or **User** bookmarks by group, or individually.
6. For each bookmark you choose to include, you can choose options from the *Bookmark* section on the right. Options include:
   - *Include email attachments*
     - This setting applies to all email children, not only common attachments.
     - Selecting this setting activates the **Export Options** button.
   - *Export files & include links*
     - Selecting this setting activates the **Export Options** button.
   - *Export Cerberus analysis html files*
   - *Include thumbnail for each object*
7. Choose a *Thumbnail Arrangement* option for each bookmark or bookmark group as follows:
   - *Number of thumbnails per row*
   - *Include all thumbnails at end of each bookmark section*
   - *Group all file paths at the end of thumbnails*
8. Specify if you want to export the bookmarked files and include links to them in the report when it is generated.
9. Specify if you want to include graphic and video thumbnails that may be part of any bookmarks. If you want to create links to original files in the report, choose both to export the original files and to include graphic and video thumbnails when the report is generated.
10. In the *Report Options* dialog, click **Bookmarks**.
11. Click **Sort Options** and do the following:
    - Click the plus (+) to add a criterion, or click minus (-) to delete a criterion.
    - Click the down arrow button on the right side of each line to open the drop down of available sort columns.
    - Click **OK** to save the selected Sort Options and close the dialog.

    Note: The sort options you see are determined by the Columns Template you have selected

    For more information on customizing columns, see Customizing File List Columns (page 481).

12. Specify if you want to apply all settings for this bookmark to child files.

Bookmark Export Options

The *Bookmark Export Options* dialog contains the following three options:

- *Link to exported email attachments and filter out attachments in bookmark*
  - When selected, this option creates links to exported email attachments and filters out the attachments in the bookmark.
- *Include re-constructed web pages*
  - When selected, this option exports all of the files necessary to view re-constructed web pages. The files are stored in the **Report_Files** folder in a sub folder called **reconstructedpage**.
- *Export selections as their own file*
  - When selected, this option saves each bookmark selection as an individual file.

Adding Graphics Thumbnails and Files to a Report

The *Graphics* section in the Report Options dialog lets you define whether-or-not to create a section in the report that displays thumbnail images of the case graphics. You can also link the thumbnails to a full sized version of the original graphics if desired.

For information about other items you can define for a report, See Creating a Case Report (page 487).

To add graphics thumbnails and files to a report

1. In the *Examiner*, click **File > Report**.
2. In the left pane, under *Report Outline*, highlight **Graphics** to display the *Graphics* options in the right pane.

   You can select the **Graphics** check box to include graphics in the report. You can deselect the **Graphics** check box to exclude graphics from the report.
3. To apply a filter to any included graphics files in a report, click **Filter** and select a filter to apply to the graphics.
4. To export and link full-sized graphics in the report, click the **Export and link full-size graphics to thumbnails** option.
5. Select one of the following options
   - **Include checked graphics only**
   - **Include all graphics in the case**
6. To sort the graphics by name or by path, click **Sort Options**. In the *Sort Options* dialog, use the Plus (+) and Minus (-) buttons to add and remove sort options. Click the drop-down arrow on the right side of the line to select either **Name** or **Path**.
7. Specify the number of graphics thumbnails to display per row and choose whether-or-not to **Group all filenames at end of report.**

Adding a Video to a Report

The Video section in the Report Options dialog lets you define lets you define whether-or-not to create a section in the report that displays the thumbnail images and/or the rendered MP4 files of the case videos. You can also choose to include a link to the original full sized version of the video. These thumbnails and MP4 videos are created during evidence processing or during additional analysis.

See Generating Thumbnails for Video Files (page 327).

See Creating Common Video Files (page 328).

To add video thumbnails and files to a report

1. In the *Examiner*, click **File > Report**.
2. In the left pane, under *Report Outline*, highlight **Videos** to display the *Video* options in the right pane.

   You can select the **Videos** check box to include videos in the report. You can deselect the **Videos** check box to exclude videos from the report.
3. To apply a filter to any included video files in a report, click **Filter** and select a filter to apply to the videos.
4. To export and link the original videos in the report, click the **Export and link original videos** option.
5. To include a link to the rendered MP4 videos that were created during evidence processing or during additional analysis, check **Export rendered videos**.
6. To include the thumbnails of the videos in the report that were created during evidence processing or during additional analysis, check **Export rendered thumbnails**.
7. Select one of the following options
   - **Include checked videos only**
   - **Include all videos in the case**
8. To sort the videos by name or by path, click **Sort Options**. In the *Sort Options* dialog, use the Plus (+) and Minus (-) buttons to add and remove sort options. Click the drop-down arrow on the right side of the line to select either **Name** or **Path**.
9. Specify the number of video thumbnails to display per row in the *Rendered Thumbnail Arrangement* group box.
10. Click **Columns**. In the *Manage Column Settings* dialog, select the Settings Template to copy or edit.

    For detailed information on creating and modifying Columns Templates, see Customizing File List Columns (page 481).

Adding a File Path List to a Report

The *File Paths* dialog lets you create a section in the report that lists the file paths of files in selected categories. The *File Paths* section displays the files and their file paths; it does not contain any additional information.

For information about other items you can define for a report, See Creating a Case Report (page 487).

To add a File Path List to a Report

1. In the *Examiner*, click **File > Report**.
2. In the left pane, under *Report Outline*, highlight **File Path** to display the *File Path* options in the right pane.

   You can select the **File Path** check box to include a file path section in the report. You can deselect the **File Path** check box to exclude a file path section from the report.
3. Select a filter from the *Filter* drop-down, to apply a filter to the items you want to include a file path list. You can leave the filter option empty to not apply a filter.
4. Select from the *Available Categories* list to include the category or categories in the report by dragging the category to the *Selected Categories* list.
5. To also export and link to the selected files in the File Path list, select the check-boxes box next to the items in the *Selected Categories* box.

   If you do not select a check-box *Selected Categories* list, the File Path is included in the report, but the files themselves are not exported and linked to the *File Path* in the report.

Adding a File Properties List to a Report

The *File Properties* dialog lets you create a section in the report that lists the file properties of files in selected categories. Several options let you make the *File Properties List* in the report as specific or as general as you want it to be.

For information about other items you can define for a report, See Creating a Case Report (page 487).

To Add a File Properties List to a Report

1. In the *Examiner*, click **File > Report**.

   In the left pane, under *Report Outline*, highlight **File Properties** to display the File Properties options in the right pane.

   You can select the **File Properties** check box to include a file properties section in the report. You can deselect the **File Properties** check box to exclude a file properties section from the report.
2. Either click the **Filter** drop-down arrow and selecting the desired filter, or choose no filter by selecting the blank entry at the top of the filter drop-down list.
3. Drag and drop the categories that you want to include from the *Available Categories* window into the *Selected Categories* window.
4. Check a category in the *Selected Categories* window to export related files and link them to the *File Properties* list in the report.

   Checking an item automatically selects the files and folders under it. If you do not want to include all sub-items, expand the list and select and deselect each item individually.
5. In the *Report Options* dialog, click **File Properties**.
6. In the *File Properties* options area, click **Columns**.
7. In the *Manage Column Settings* dialog, select the Settings Template to copy or edit.

   For detailed information on creating and modifying Columns Templates, see Customizing File List Columns (page 481).
8. When you are done defining the columns settings, click **OK**.

   You might want to define how the data is sorted, according to column heading. In the *File List* view you are limited to a primary and secondary search. In the Report wizard, you can define many levels of sorting.
9. In the *Report Options* dialog, click **File Properties**.
10. In the *File Properties* options area, click **Sort Options** and do the following:
    - Click the plus (+) to add a criterion, or click minus (-) to delete a criterion.
    - Click the down arrow button on the right side of each line to open the drop down of available sort columns.
    - Click **OK** to save the selected Sort Options and close the dialog.

    Note: The sort options you see are determined by the Columns Template you have selected

    For more information on customizing columns, see Customizing File List Columns (page 481).

Adding Registry Selections to a Report

If your drive image contains Registry files, you can include them in your report.

When creating a Report that includes Registry files, a **DAT** extension is being added to the link. If the link does not open in the report, it can be exported and opened in Notepad.

For information about other items you can define for a report, See Creating a Case Report (page 487).

To Add Registry Selections to a Report

1. In the *Examiner*, click **File > Report**.

   In the left pane, under *Report Outline*, highlight **Registry Selections** to display the registry selections options in the right pane.

   You can select the **Registry Selections** check box to include a Registry Selections section in the report. You can deselect the **Registry Selections** check box to exclude a Registry Selections section from the report.
2. In the *Registry File Types* window, check the file types for which you want to include headings for in your report.
3. In the right window, check the registry file paths that you want included in your report.
4. Mark the box **Include user generated reports (if any)** if you have generated Registry Reports using Registry Viewer, and you want to include them in this report.

   Note: User-generated reports must exist in the case before generating the report, otherwise, this option is disabled. These reports are generated in Registry Viewer and can be collected from the Registry data found on the source drive.
5. Mark the box **Select Auto Reports**, to view and select which registry reports to include in the report from those that were generated automatically based on the registry reports selection in *Case Manager* **> Case > New > Detailed Options > Evidence Refinement**.

   Note: If you did not select this option during pre-processing, this option is disabled in the *Report Options* dialog.

Adding Screen Captures from Examiner

You can now capture screen shots within the Examiner interface. You can include the screen captures when creating reports. You can use screen captures to include information that is not easy to export or include in reports, such as:

- The contents of the Natural view (File Content pane)
- The contents and information in the File List
- The contents of visualization pages

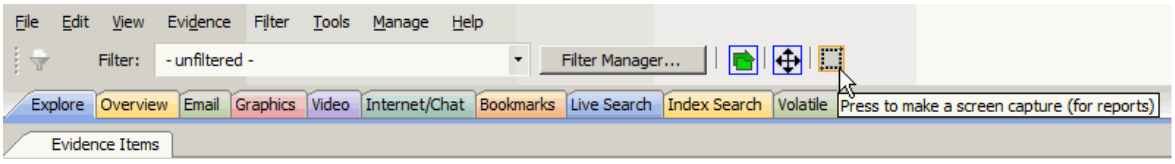
These UI elements can include information that is useful as evidence, but there is no way to present it outside of the UI.

When you create a screen capture, the following occurs:

- The file is saved in the case folder under a **Screenshots** sub-folder. (Do not manually rename the captured files, otherwise the Report dialog will not find them.)
- The file is saved in the original size and in a smaller size that may be needed to fit in a report.
- The name and description of the file is saved in the database so that they can be displayed in the *Report Options* dialog.

To create a screen capture

1. In the *Examiner*, click the screen capture icon.



2. Click and drag the + cursor to select the area that you want to capture.
3. In the *Screen Capture Info* dialog, give the screen capture file a name.
4. Enter a description.
   This is recorded with the filename in the database.
5. Click **Save**.
6. To cancel a screen capture, click Esc.

To include a screen capture in a report

1. In the Examiner, click **File** > **Report**.
2. In the *Report Options,* click **Screen Capture**.
3. Select the screen captures that you want to include in the report.
4. (Optional) You can edit the description of the files, but not the filename.
5. Configure the other options for the report.
   When the report is created, the image files are copied to the report folder.

Selecting the Report Output Options

The *Report Output* dialog lets you select the location, language, report formats, and other details of the report. You can also recreate the directory structure of exported items.

For information about other items you can define for a report, See Creating a Case Report (page 487).

To select the report output options

1. When you have completed defining the report, from the *Report Options* dialog, click **OK** to open the *Report Output* options dialog.
2. Type the destination folder name for the saved report, or use the *Browse* button to locate and select a location.
3. Use the drop-down arrow to select the language for the written report. Available languages are as follows:

Arabic (Saudi Arabia)	Chinese (Simplified, PRC)
English (United States)	German (Germany)
Japanese (Japan)	Korean (Korea)
Portuguese (Brazil)	Russian (Russia)
Spanish (Spain, Traditional Sort)	Swedish (Sweden)
Turkish (Turkey)	

4. Indicate the formats for publishing the report. You can choose any or all of the output formats.

   To view a report made in any of the supported formats, you must have the appropriate application installed on your computer. Options are as follows:

PDF (Adobe Reader)	HTML (Windows Web Browser)
XML (Windows Web Browser)	RTF (Rich Text Format: Most Text Editors)
WML (Unix Web Browser)	DOCX (MS Office Word 2007)
ODT (Open Document Interchange: Sun Microsystems OpenOffice Documents)	
Load File	

Note: Some report output formats require J#, either 1.1 or 2.0. If you select RTF format, for example, and J# is not installed, you will see an error.

5. Under Export Options do the following:
   - Check the *Use object identification number for filename* to shorten the paths to data in the report. Links are still created for proper viewing of the files.
   - The unique File ID numbers, when used in a report, keep the pathnames shorter. This makes burning the report to a CD or DVD more reliable.
   - Check the *Append extension to filename if bad/absent* box to add the correct extension where it is not correct, or is missing.

6. Under HTML Report Customization, choose from the following:
   - If you wish to use your own custom graphic or logo, mark the *Use custom logo graphic* box, then browse to the file and select it. Use GIF, JPG, JPEG, PNG, or BMP file types.
   - If you wish to use a custom CSS file, mark the **Use custom CSS** box. Select the folder where the custom CSS files have been saved. Click **OK**. The folder you selected displays in the "Use Custom CSS" text box.
7. Click **OK** to run the report.

   If the report folder you selected is not empty, you will see the following error message:

   Choose to **Delete** or **Archive** the contents of the folder, or to **Cancel** the report. Delete the contents of the current destination folder, or change to a different destination folder, then recreate the report or import it if you saved it during creation.

Creating a Load File

It is possible to create a load file, which enables you to export data from an existing or new case and import it into ligitation document management applications such as AccessData Summation and eDiscovery.

To Create a Load File

1. In the *Examiner*, click **File > Report**.
2. In the left pane, under the *Report Outline*, select the check boxes for the options you would like to include in your load file. Be sure to highlight each item selected and fill out the appropriate information. You can add information to these areas using the methods described in the previous segments. When finished, press **OK**.
3. In the *Report Output* dialog, enter the path to the *Report Folder*. This is where your report will be located.
4. Select the appropriate *Language* and *Time Zone*.
5. Select the correct *Export Option*. Options include:
   - *Use object identification number for filename*
     - This setting makes it so the object identification number used in the exising or new case is also used as the filename in the load file.
   - *Append extension to filename if bad/absent*
     - Selecting this setting will append the correct or assigned filename to a file if none is present or if the current one is bad.
6. In the *Formats* area, check the box next to *Load File* and click the **Options** button.
7. In the *Load File Export Options* dialog, enter a *Load File Name*.
8. Select a *Format* for your load file. Options include:
   - *Browser Briefcase*
     - This option generates an HTML format that provides links to the native documents, images, and text files. You can have multiple links for image, native, and text documents. You can also work with production sets exported previously in iBlaze Browser Briefcase format. This allows you to have greater control over the production set.
   - *CaseVantage*
     - This option generates a DII file specifically formatted for use with the AD Summation CaseVantage program.
   - *Concordance*
     - This option generates a DAT file that can be used in Concordance.
   - *EDRM*

    - This option generates an XML file that meets the EDRM v1.2 standard.
- *Generic*
    - This option generates a standard delimited text file.
- *iCONECT*
    - This option generates an XML file formatted for use with the iConect program.
- *Introspect*
    - This option generates an IDX file specifically formatted for use with the Introspect program.
- *Relativity*
    - This option generates a DAT file that can be used in Relativity.
- *Ringtail (MDB)*
    - This option generates a delimited text file that can be converted to be used in Ringtail.
- *Summation eDII*
    - This option generates a DII file specifically formatted for use with the AD Summation iBlaze or Enterprise programs.

Note: If you are outputting a Concordance, Relativity, or Generic load file, and include rendered images, you will also get an OPT and LFP file in the export directory.

9. Choose an *Encoding* option for your load file from the following:
    - *ANSI*
    - *UTF-8*
    - *UTF-16*
10. If you are creating a Concordance, Generic, Introspect, or Relativity load file, you need to specify the following options:
    - Choose whether to *Include a Header Row* by clicking on the checkbox.
    - Select the *Multi-Entry Separator*.
    - Select the *Field Mapping*.
    - Select the *Text Identifier*.
    - Select the *Newline*.
11. For the Browser Briefcase, CaseVantage, EDRM, iConect, Ringtail, or Summation eDII options, select only the *Multi-Entry Separator*.
12. In the *Available Fields* pane, select the options you want to appear in your report. Highlight each field you would like to include and click the **>>** button to move it to the *Selected Fields* pane. If you would like to change the order of appearance for these items in the report, highlight the item you would like to move in the *Selected Fields* pane and click on the **Up** or **Down** button until it is in the right place.
13. The *Files To Include* tab contains the following three options:
    - *Export Native Files*

    When selected, this option allows you to export the emails contained in PST/NSF in one of three different ways:
        - *OUtput a reduced version of the original PST/NSF file*
        - *Output messages as individual HTML/RTF files*
        - *Output messages as individual MSG files*
    - *Export Rendered Images*

    When selected, this option allows you to select how rendered images appear in the load file. You can export using one or both of the following options:
        - *Use existing image*

- *Use SWF image*

You can also select the *File Format* and *Page Size* for displaying these images.

- *Export Text*

When selected, this option allows you to choose the *Export Priority* from the following options:

- *Export extracted text over OCR text*
- *Export OCR text over extracted text*
- *Export both extracted text and OCR text*

14. When finished selecting these options, click **OK** in both the *Load File Export Options* and *Report Output* dialogs.
15. The progress of load file generation will appear in the *Data Processing Status* dialog. Once the load file is generated, you can find it in the folder entered in Step 3. This folder will contain the load file as well as the original files for any items included in the report.

Note: Best results occur when you select the Summation defaults and the *Enable Standard Viewing* feature during processing when creating the case.

Customizing the Report Graphic

When you select HTML as an output format, you can add your own graphic or logo to the report.

To add your own graphic or logo

1. In the *Examiner*, click **File > Report** to open the Report wizard.
2. From the *Report Options* dialog, after you are done making selections for the Report Outline, click **OK**.
3. In the *Report Output* dialog, under Formats, mark **HTML**. This activates the HTML Report Customization options.
4. Under HTML Report Customization, mark **Use custom logo graphic**.
5. Click the **Browse** button to open the Windows Explorer view and browse to the graphic file to use for the report. The file format can be JIF, JPG, JPEG, PNG, or BMP.
6. Click **Open**.
7. When all Report options have been selected, click **OK**.

   The progress bar dialog indicates the progress of the report.

   Note: When selected, the finished HTML and/or PDF reports open automatically.

   You can process only one set of reports at a time. If you select the options to create several different report formats before clicking **OK** to generate the report, all will process concurrently. However, if you start that process and then decide to create a new report, you will not be able to until the current report is finished generating.

   If you start another report too soon, you will be prompted to wait, if you chose to create either HTML or PDF format for the report, it will automatically open when creation is complete. Otherwise, to view the report, click **Yes** when prompted.

Using Cascading Style Sheets

The formatting of reports can be customized with Cascading Style Sheets (CSS). Reports stores a file path you select (default or custom) to the folder containing the custom CSS files. When CSS is not selected, Reports use the default settings.

For reports to utilize the cascading style sheets, three CSS files are necessary, and must all be located in the specified CSS folder:

- Common.CSS
- Bookmarks.CSS
- Navigation.CSS

The original CSS files are found in the following path if no changes were made to the default:

C:\Program Files\AccessData\Forensic Toolkit\<version>\bin\ReportResources

Copy the *CSS files to a different directory before making changes to any of these files. Do not make changes to the original files.

To utilize the customized CSS files, click **Use custom CSS**, and select the path to the folder where the customized CSS files are stored.

When CSS is selected, Reports checks for those files in the specified directory. If any of the three files is missing you are notified and the report does not proceed.

Note: The UI option consists of a check box and a text path string. The path string points to the path directory that contains the three needed CSS files.

Note: The UI options settings are persistent per Windows login user. Thus, your selections will be persistent across the Case List for the currently authenticated user.

Important: In versions, the cascading style sheets have been updated for a better user experience. Updates include persistent highlighting on the navigation tree (so examiners know which item they are viewing) and better organization of data within the report.

However, if you have created personalized templates in previous versions, you will need to re-create them for 5.1.

Viewing and Distributing a Report

The report contains the information that you selected in the Report Wizard. When included in the report, files appear in both raw data and in the report format.

To view the report outside of Examiner

1. Browse to the report file
2. Click on the report file:
   - Click on index.htm to open an HTML document in your Web browser.
   - Click on the file [*report*].PDF to open the report in a PDF viewer.

Modifying a Report

Modify the report by changing the report settings, and recreating it. Add the new evidence or change report settings to modify the report to meet your needs.

Change the report settings for each report as needed.

All previously distributed reports should be retracted to keep all recipients current.

Note: If you want to keep a previous report, save the new report to a different folder that is empty.

Exporting and Importing Report Settings

Report settings are automatically saved whenever you generate a report. You can export the settings that you used as an XML file. You can then later import and reapply those same settings to use with new reports that you generate.

To export report settings

1. In the *Examiner*, click **File > Report**.
2. In the *Report Options* dialog box, click **Export**.
3. In the *Export Sections* dialog, select the sections that you want to export.
4. Click **OK**.
5. Click **Browse** to select a folder to save the settings.
6. You can accept the default name for the report settings file, or you can type a name for the settings file. An XML extension is automatically added when the report is created.
7. Click **Save** for each item you have selected in the Report Outline list.
8. Click **OK**.

To import saved settings for a new report

1. In the *Examiner*, click **File > Report**.
2. In the *Report Options* dialog, click **Import**.
3. Browse to a settings XML file that you want to apply, and select it.
4. Click **Open** to import and apply the settings file to your current report.

Writing a Report to CD or DVD

You can write a report to a CD or DVD, depending on the report's size. It is recommended that you select **Use object identification number for filename**, in the *Report Output* options dialog. This option keeps paths shorter, so they do not exceed the limits of the media format.

After you create the report, write only the contents from the root of the report folder, and not the report folder itself. The autorun automatically launches the report's main page (index.htm) using the default browser when the CD is read on a Windows computer.

Note: The following information pertains to burning reports to a CD or DVD.

- When burning some reports to a CD, some Registry Viewer Auto Reports links may be broken, where they work when viewing on the computer. To avoid this issue, make sure that longer Joliet filenames are enabled when burning report to a CD.
- To launch the report, the computer must be configured to automatically execute autorun files.
- If you burn the folder that contains the report to the CD or DVD, the autorun will not be at the root of the disk, and will not work properly.
- To prevent broken links to report files, use File Item numbers instead of names to keep paths short, and / or use the Joliet file naming to allow longer file paths.

Part 6

Reference

This part contains additional reference information and contains the following appendices

- Working with Windows Registry Evidence (page 528)
- Supported File Systems and Drive Image Formats (page 537)
- Recovering Deleted Material (page 540)
- Managing Security Devices and Licenses (page 542)
- Configuring a Multi-box Setup (page 561)
- AccessData Distributed Processing (page 565) AccessData Oradjuster (page 572)

Chapter 37

Installing the AccessData Elasticsearch Windows Service

About the Elasticsearch Service

The AccessData Elasticsearch Windows Service is used by multiple features in multiple applications, including the following:

- KFF (Known File Filter) in all applications
- Visualization Geolocation in all applications

The AccessData Elasticsearch Windows Service uses the Elasticsearch open source search engine.

Prerequisites

- For best results with eDiscovery products and AD Lab and Enterprise, you should install the AccessData Elasticsearch Windows Service on a dedicated computer that is different from the computer running the application that uses it.

  For single-computer installations such as FTK, you can install the AccessData Elasticsearch Windows Service on the same computer as the application.

  A single instance of an AccessData Elasticsearch Windows Service is usually sufficient to support multiple features. However, if your network is extensive, you may want to install the service on multiple computers on the network. Consult with support for the best configuration for your organization's network.
- You can install the AccessData Elasticsearch Windows Service on 32-bit or 64-bit computers.
- 16 GB of RAM or higher
- Microsoft .NET Framework 4

  To install the AccessData Elasticsearch Windows Service, Microsoft .NET Framework 4 is required. If you do not have .NET installed, it will be installed automatically.
- If you install the AccessData Elasticsearch Windows Service on a system that has not previously had an AccessData product installed upon it, you must add a registry key to the system in order for the service to install correctly.

Installing the Elasticsearch Service

Installing the Service

To install the AccessData Elasticsearch Windows Service

1. Click the AccessData Elasticsearch Windows Service installer.

   It is available on the KFF Installation disc by clicking *autorun.exe*.
2. On the welcome page, click **Next**.
3. Accept the License Agreement and click **Next**.
4. If you do not have Java installed, a message is displayed stating that you must install Java and the installation will end. See Prerequisites on page 511.
5. If you have upgraded your Java, you will get a Path Mismatch dialog. This asks you if you want to change the path of the JAVA_HOME variable to you new Java version. Click **Yes.**
6. On the *Destination Folder* dialog, click **Next** to install to the folder, or click **Change** to install to a different folder.

   This is where the Elasticsearch folder with the Elasticsearch service is installed.
7. On the *Data Folder* dialog, click **Next** to install to the folder, or click **Change** to install to a different folder.

   This is where the Elasticsearch data is stored.

   Note: This folder may contain up to 10GB of data.
8. Configure *User Credentials.*

   (For use with KFF) In the *User Credentials* dialog, you can configure credentials that the Elasticsearch service uses to access network shares. This is used when either importing KFF Data files, or when exporting KFF binary files.

   You have two options:

   - Local System Account - This option uses the Local System account. If you select this account, you can import files from and export files to a share that is accessible only to this local account. For example, with this option selected, you could export a binary only to a local share that this account can access. If you select the Local System Account, do not enter any domain value, such as localhost. Leave it blank instead.
   - Specified User Account - This option lets you specify a specific domain user account. If you select this account, you can import files from and export files to a network share that is available to the user. For example, with this option, you could export a binary to a share on a different computer. To use this option, enter the user name, the domain name, and the password.

   After installation, you can view and modify this setting by doing the following:

   - Open the Services window. The services window shows you the account that the service is logged in as. If the window doesn't show the column, you can add the column to the window.
   - You can right-click the service and select properties to have the option to change the account that the service has logged in as. The service has to be stopped first, and the restarted, in order to make a change.
9. In the *Allow Remote Communication* dialog, you can scale Elasticsearch by adding more machines.

   (Optional) Select Enable Remote Communication.

   Note: If Enable Remote Communication is selected, a firewall rule will be created to allow communication to the AccessData Elasticsearch Windows Service service for every IP address

added to the IP Address field. If no IP addresses are listed, then ANY IP address will be able to access the AccessData Elasticsearch Windows Service.

Either leave blank or add machines and click **Next**.

10. Configure ports for Elasticsearch to use and click **Next**.
    - HTTP Port
    - Transport Port

    You can use the default ports or specify your own.

    Using the defaults, whenever you click *Next*, the system will determine if the ports are available. If one is in use, a new value will automatically be entered. Click **Next** again to verify the ports and continue.

11. The *Configuration 1* dialog contains the following fields:
    - **Cluster name** - This field automatically populates with the system's name.
    - **Node name** - This field automatically populates with the system's name.

    Note: If installing the AccessData Elasticsearch Windows Service on more than one system, allow the first system to install with the system's name in the cluster and the node fields. In the second and subsequent systems, enter the first system's name in the cluster field, and in the node field, enter the name of the system to which you are installing.

    - **Heap size** - This is the memory allocated for the AccessData Elasticsearch Windows Service. Normally you can accept the default value. For improved performance of the AccessData Elasticsearch Windows Service, increase the heap size.
12. The *Configuration 2* dialog contains the following options:
    - **Discovery** - Selecting the default of *Multicast* allows the AccessData Elasticsearch Windows Service search to communicate across the network to other Elasticsearch services. If the network does not give permissions for the service to communicate this way, select *Unicast* and enter the IP address(es) of the server(s) that the AccessData Elasticsearch Windows Service is installed on in the *Unicast* host names field. Separate multiple addresses with commas.
    - **Node** - The Master node receives requests, and can pass requests to subsequent data nodes. Select both Master node and Data node if this is the primary system on which the AccessData Elasticsearch Windows Service is installed. Select only Data node if this is a secondary system on which the AccessData Elasticsearch Windows Service is installed. Click **Next**.
13. In the next dialog, click **Install**.
14. If the service installs properly, a command line window appears briefly, stating that the service has installed properly.
15. At the next dialog, click **Finish**.

Troubleshooting the AccessData Elasticsearch Windows Service

Once installed, the AccessData Elasticsearch Windows Service service should run without further assistance. If there are issues, go to **C:\Program Files\Elasticsearch\logs** to examine the logs for errors.

Chapter 38

Installing the Windows Agent

This chapter covers the manual installation of the agent in a Windows environment.

This chapter includes the following topics:

- See Supported Hashing Algorithms on page 514.
- See Manually Installing the Windows Agent on page 514.
- See Using Your Own Certificates on page 520.

Running the AccessData Agent on Windows 8 and 10 is now supported.

Important: The following FTK and Enterprise features are not supported for target computers running Windows 8 and 10:

- Memory Analysis
- Import Memory Dump
- Volatile Memory

Supported Hashing Algorithms

The certificates used by agent and site server can use either the SHA-1 or SHA-256 hashing algorithm. These do not require any “Key Usage” or other special fields.

Manually Installing the Windows Agent

Perform the following steps to manually install the Enterprise Agent in Windows:

- Specific Instructions for eDiscovery (page 514)
- Specific Instructions for AD Enterprise (page 515)
- Installing the Agent (page 516)
- Configuring Execname and Servicename Values (page 518)

Specific Instructions for eDiscovery

Follow these instructions if installing the Windows agent for use in eDiscovery.

A certificate (both a public certificate and a private certificate) is required for secure communication with agents.

Configuring the Work Manager for the private certificate to use with Site Server

1.
2. Navigate to %\Program Files\AccessData\eDiscovery\Work Manager
3. In Notepad or some other text editor, open **Infrastructure.WorkExecutionServices.Host.exe.config**.
4. Go to the line:
   <add key="SSAgentCertFile" value="*path*" />
5. Enter the path of your file.
6. Go to the line:
   <add key="SSCommunicationCertPath" value="*path*" />
7. Enter the path of your file.
8. Save the file.

Specific Instructions for AD Enterprise

Follow these instructions if installing the Windows agent for use in AD Enterprise.

Preparing the AD Enterprise Agent Certificate

About Enterprise Security Certificates:

When installing AccessData Enterprise *Examiner*, you need a security certificate. Enterprise Management Server creates Enterprise security certificates, the CRT public key and the PEM public and private key pair files. However, the Enterprise Configuration Management Tool now also accepts PKCS#12 certificates.

If you have a third-party certificate chain in the PKCS#12 format, the Enterprise Configuration Management Tool reads the PKCS#12 certificate and asks for the user password. The certificate is decrypted only long enough to gather the information necessary for the Enterprise installation, then re-encrypts the private key. The public key, regardless of source, must be in standard binary or base-64 encoding.

If the Agent is installed, or pushed, to the workstations using Enterprise, the certificate information will automatically be read from the Enterprise Configuration Management Tool. If the Agent is pushed out, the certificate information (paths and filenames) must be re-entered. The public certificate itself must be in an area of the network where it can be accessed by the Agent machine during installation, but does not need to be stored on the Agent machine.

In addition, the Agent uses only a public key. As long as that public key is in binary or base-64 format, it will automatically be read by the Agent. For more information, see Using Your Own Certificates (page 520).

To prepare the certificate

1. Prepare the Agent Certificate.
2. Copy the needed certificate from the Management Server to your deployment location.
   Management Server creates certificates during the setup in:
   [*Drive*]:\Program Files\AccessData\AccessData Management Server\certificates.
   The certificate name is the **ManagementServer.crt**.

3. Copy **ManagementServer.crt** to a folder of your choice where it can be accessed while installing the Agent.

Installing the Agent

To install the Agent

1. Run **AccessDataAgent.msi** or **AccessDataAgent(64bit)** using **msiexec**.

   Note: These .msi files are located in the Program Files\AccessData\Forensic Toolkit\5.1\Bin\Agent\<x32 or x64> folder after installation.

   There are several command line parameters available to use with this **.msi** as documented below. Here is an example command line that will install with the defaults:

   If **AccessDataAgent.msi** resides in the folder **C:\enterprise** and **ManagementServer.crt** resides in [*Drive*]**:\certificates**, type the following command line to install the agent with defaults:

   msiexec /i [*Drive*]:\enterprise\AccessDataAgent.msi CER=[*Drive*]:\certificates\ManagementServer.crt.

The following table lists the command line options available for use with this **AccessDataAgent.msi:**

Command Line Options

Option	Action
/i (i or x required)	Specifies install.
/x (i or x required)	Specifies un-install.
/qn (optional)	Allows you to install in quiet mode with no user interaction.
<path and msi file name> (required)	If running from the folder where the .msi is located you do not have to include path, only the filename.
CER=<path and certificate file name> (required)	Specifies the certificate the agent uses. *Always include the path, regardless of location.*
ALLUSERS=<*n*>	Configures the installer to be available to all users. The default option varies per operating system. The options are: • *allusers=1* configures the installer to be available to all users. • *allusers=0* configures the installer to be available to only the user who is installing the agent.
INSTALLDIR=<custom install path> (optional)	Allows you to change the install location from the default folder: (C:\Program Files\AccessData\Agent).
PORT=<**xxxx**> (optional)	Allows you to change the port from the default port (3999).
LIFETIME=<**d**> (optional)	Allows you to configure the life cycle of the agent. The "**d"** value equals the Time To Live (TTL) measured in days. Adding a number preceded by a dash measures the TTL in minutes. For example: <-*d* >.
CONNECTIONS=<n>	Allows you to configure the number of maximum connections for the agent.

Command Line Options (Continued)

Option	Action
STORESIZE=<n>	Allows you to configure the size of the data store.
TRANSIENT=1	Allows you to configure the agent as a *Transient Agent*. Transient Agents have no protected storage and remove themselves when the agent machine is restarted.
FOLDER_STORAGE=1	Allows you to configure the agent as a *Persistent Agent*. Persistent Agents use a “local” file system based storage and not protected storage. Persistent Agents also remain on the agent machine after the machine is restarted. This allows for local logical disc space to store the results of Public Site Server jobs operating while the Agent is not on the WAN or can get to the Public Site Server.
SERVICELESS=1	Allows you to configure the agent to install with no protected storage and no installed service. The agent removes itself when the agent machine restarts or when the lifetime option expires, whichever comes first.
PCD=<*x* > (optional)	**Enterprise Only:** Allows you to configure the Proxy Cycle Delay (PCD). The PCD is the time interval at which the agent attempts to connect to proxy to check if any work has been assigned. The PCD “*x*” value is measured in seconds. The default is 1200 (20 minutes).
PROXY= (see example below) (optional) <PrimaryIP>,<SecondaryIP>:<Port>~<PrimaryIP2>,<SecondaryIP2>:<Port2>	**Enterprise Only:** Allows you to configure a proxy-able agent. PrimaryIP should refer to the IP address to which the agent should try to communicate. (Usually this will be the internal private network IP of the proxy server.) The “SecondaryIP” should refer to the IP address to which the agent should try to connect when the attempts to connect to the “PrimaryIP” have failed. (Often this IP will represent the public IP of the proxy server.) PrimaryIP2 and SecondaryIP2 should refer to an additional proxy server address and is delimited by a tilde (~). Additional proxy servers can be added by following this same pattern.
MAMA=<Site Server IP address:port>	**eDiscovery Only:** Allows you to configure the IP Address of the Site Server to which the agent reports. For example, 10.32.41.113:54545 This parameter is used so that the Agents know which Site Server to check into for the first time. Additionally, after that first check-in, the Agents will learn the Site Servers that has its CIDR and check there next time. It will update based on movement of the physical IP of the node.

Command Line Options (Continued)

Option	Action
PUBSS=<public instance IP>	**eDiscovery Only:** Allows you to configure the agent to connect to a Public Site Server (PUBSS). See About Site Servers on page 536. For example, pubss=192.192.192.192:5432 The Agent in Public Site Server (PUBSS) mode will check-in to the original PUBSS value that was part of the install. After that first check-in, it will receive a list of other Public Site Servers in the DMZ and then ping around to find the closest/fastest connection. For example, if the user is in New York and a job starts there, and then the user goes to Los Angeles, the user will go from the NYC PUBSS to the LA PUBSS and the collection should resume and support interruption. This is all completed based on the resolution of the IP address for the target and assignment in a proper CIDR range on Site Server config. See Site Server Configuration on page 539. This list will also get updated whenever it might change. This list comes from the Site Server configuration parameters you setup on your internal servers and not specifically some additional data entry. It comes from the virtue of having any Public Site Servers deployed. See MAMA=<Site Server IP address:port> on page 517.
PUBSS_DELAY=<seconds>	**eDiscovery Only:** This can be used to delay the default check-in interval (30 minutes). You may want to alter this value if you have a lot of Agents on the PUBSS system.

Example Command Line Install

msiexec /i "C:\AgentInstall\AccessData Agent (64-bit).msi" cer="C:\AgentInstall\AccessData E1.crt" mama=10.10.35.32:54545 TRANSIENT=1 Persistent=1 Serviceless=1 lifetime=1 or lifetime=-5 pubss=192.192.192.192 5432

Configuring Execname and Servicename Values

The Execname and Servicename values change the names of the agent executable and agent service respectively. These values are added to the MSI using an MSI editor (such as **ORCA.exe** — a free MSI editor).

Changing the Execname Value

To make changes to the execname value

1. Run **Orca.EXE**.
2. Click **File > Open**.

3. Browse to the folder containing the "AccessData Agent.msi" or "AccessData Agent (64-bit).msi" file and open the file. The default path is:

   [*Drive*]:\Program Files\AccessData\Forensic Toolkit\3.2\Bin\Agent\x32 (or x64)\

4. In the *Tables* list, select **File**...
5. In the *FileName* column, double-click "u4jwdc7h.exe|agentcore.exe".

   5a. Enter the filename to use for the agent core executable.

   Note: Replace the entire string with the filename.

6. Press **Enter**.
7. Click **File > Save.**

Note: Do not close Orca if you are also changing the service name.

Changing the Servicename Value

To make changes to the Servicename value

If you closed Orca, begin with Step 1. Otherwise, skip to Step 4.

1. Run Orca.EXE.
2. Click **File > Open**.
3. Browse to the folder containing the "AccessData Agent.msi" or "AccessData Agent (64-bit).msi" file and open the file. The default path is:

   [*Drive*]:\Program Files\AccessData\Forensic Toolkit\3.2\Bin\Agent\x32 (or x64)\

4. In the *Tables* list, select "*ServiceControl*".
5. In the *Name* column, double-click "*AgentService*".

   5a. Enter the name to use for the *AgentService* and press **Enter**.

   Note: Use the same value in steps 5a, 7a and 8a.

6. In the *Tables* list, select "*ServiceInstall*".
7. In the *Name* column, double-click "*AgentService*".

   7a. Enter the name to use for the *AgentService* (use the same value entered in step 5a) and press **Enter**.

8. In the *DisplayNam*e column, double-click "*AgentService*".

   8a. Enter the name to use for the *AgentService* (use the same value entered in steps 5a and 7a) and press **Enter**.

9. Click **File > Save.**
10. Click **File > Close**.

Using Your Own Certificates

Use this information if you are using your own of the following certificates:

- PKCS#12: Standard certificate packaging to securely transfer public/private key pairs
- PKCS#7: Standard certificate package to store certificates for S/MIME encryption--used for storing sets of public key chains.

Important:

- A CER/CRT public certificate must be in Base64 format (not binary DER).
- A P7B public certificate must be in binary DER (not Base64) format.
- If using a P7B, make sure it includes the top-level certificate. (It may be easiest to just make sure it includes the full certificate path.)

To export the public certificate when using a PFX (PKCS#12) key

1. Using the PKCS#12 provided by the Certificate Administrator, double-click PKCS#12 to open it.
2. Install the certificate into a local Microsoft certificate store by following the wizard supplied when you double-click the certificate file.
3. View the public certificate of the installed certificate by opening the local machine's certificate store. (This can be done with *Microsoft Management Console* or in *Internet Explorer* under **Tools > Internet Options > Content > Certificates**)
4. Find the bottom level certificate and double-click the certificate to view it.
5. Click the **Certification Path** tab to verify that the certificate has a full verification path, meaning that nothing is missing from the top of the chain to the bottom.
6. Click the **Details** tab and click **Copy to File**.
7. Click **Next** and click **Cryptographic Message Syntax Standard -** PKCS #7 **Certificates**.
8. Select **Include all certificates in the certificate path if possible**.
9. Click **Next** and enter a file export path.
10. Click **Next.**
11. Click **Finish**.
12. Double-click the exported PKCS#7 and verify that all of the public certificates in the chain are in the PKCS#7.

The exported file you created will be used as the certificate for the agent installation.

Controlling Consumption of the CPU

You can edit a registry key that allows you to control what percentage of the CPU is used for the agent. This gives you the ability to throttle the CPU and insure that the agent does not consume all of the CPU available.

To add a throttling registry key

1. In the Registry Editor, expand the HKEY_LOCAL_MACHINE hive and locate the HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Shared folder.
2. Add a new DWORD (32-bit) value to the Shared folder.(HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Shared\throttling)
3. The data value of the DWORD should be the maximum percentage of the CPU allowed to be used by the module. For example, if you want the maximum percentage of the CPU used to be 25 percent, modify the DWORD data value and enter 25 in the *Edit DWORD* dialog. The value should be from 0-100. If the data value is left at 0, the CPU will not be throttled when the agent is started.
4. In the *Edit DWORD* dialog, select the **Decimal** radio button and click **OK**.
5. After applying the registry key changes, restart the agent service.

For more information on adding and editing registry keys, see Microsoft's documentation.

Important Information

The following information is important to know about installing and executing an agent:

- The ADMON module does not run on low resource priority. The ADMON module must run on Normal priority or higher in order to maintain connection to the system drivers.

Chapter 39

Installing the Unix / Linux Agent

This chapter discusses the Unix Agent Installer. It includes the following topics:

- See Installing The Enterprise Agent on Unix/Linux on page 522.

Installing The Enterprise Agent on Unix/Linux

The AccessData Agent is available for Unix-, Linux-, and Mac-based operating systems as well as for Windows. This appendix discusses the specific installation files to use for supported Unix and Linux platforms.

Supported Platforms

The Unix Agent Installer supports the following platforms:

Unix Agent Supported Platforms

Installer	OS
	Red Hat Linux 6.x and 7.x The 6.2 Linux Agent requires GLIBC 2.17 or newer. Collection from a system running an older GLIBC version can be attempted using the 6.1 version of the Agent, which can be obtained by contacting AccessData Support. A system's GLIBC version can be determined by running the following command: ldd -version.
agent-rh5.sh or agent-rh5x64.sh	RedHat 5 (32- & 64-bit) SLED 11 (Suse Linux Enterprise Desktop) (32- & 64-bit) CentOS Enterprise 5 (32- & 64-bit) Ubuntu 9 (and newer) (64-bit)
agent-rh3.sh or agent-rh3x64.sh	RedHat 3 (32- & 64-bit) Novell Linux Desktop (NLD) 9 (32-bit) SLED 10 (Suse Linux Enterprise Desktop) (32- & 64-bit)
Be sure to use the correct installer file for your 32- or 64-bit architecture/OS)	

To install the Unix Agent

Execute the following command as root, and provide the appropriate information:
agent-<os>.sh <certpath> [-installpath| -i <installpath>]

where **<os>** is the operating system agent that is being used, and where **<certpath>** is the location of the public certificate to be used for identification, and where [**-i | -installpath**] indicates the directory to install the agent in. This defaults to:
/usr/AccessData/agent

Enterprise Unix/Linux Agent Install Parameters and Options

Option	Result
-installpath, -i <installpath>	The destination path for installing the agent. Default: /usr/AccessData/agent/.
-lifetime, -l <lifetime>	The lifetime of the agent. Default: 0.
	If <lifetime> ==0, it will never uninstall itself. If <lifetime> >0 it is days before uninstall. If <lifetime> <0 it is in minutes before uninstall.
-port, -p <port>	The port the agent listens on. Default: 3999.
-connections, -c <connections>	The maximum number of concurrent connections allowed by the agent. Default is 10.
-size, -s <storagesize>	The protected storage area size. Default is 16777216 (16 MB)

Uninstallation

To uninstall the Unix Agent, execute the following command as root:
 # ./agent.sh -rf

Configuration

The configuration file is located in the install path and is named **ADAgent.conf**. It supports the following parameters:

- **Port**: Port on which to listen for activity.
- **MinThreadCount:** Minimum number of threads to have ready, waiting for connections.
- **MaxThreadCount:** Maximum number of threads servicing connections.
- **CertificatePath**: Fully qualified network path or local path to the certificate. The installer, by default, puts the certificate in the installation path.

Starting the Service

To start the Unix Agent service, execute the following command as root:
/etc/init.d/adagentd start

Stopping the Service

To stop the Unix Agent service, execute the following command as root:

```
/etc/init.d/adagentd stop
```

Chapter 40

Installing the Mac Agent

This chapter discusses the Agent Installer for Apple Macintosh. It includes the following topics:

- See Configuring the AccessData Agent installer on page 525.
- See Installing the Agent on page 527.
- See Uninstalling the Agent on page 527.

Configuring the AccessData Agent installer

The AccessData Agent requires an X.509 certificate in order to establish a secure network connection to the server or for AD Enterprise, the computer running *Examiner*. The package installer has been provided to aid in the distribution efforts of these certificates by allowing an Administrator to modify the AccessDataAgent package installer prior to installation of AccessData Agent software for Apple Macintosh. In addition to certificate distribution, the port used by the Agent can be configured.

The following instructions allow an Administrator to configure the AccessData Agent package installer.

Bundling a Certificate

The AccessData Agent installer requires that a certificate (or certificate tree) is bundled with the installer. The following is the sequence of steps that must be followed to bundle a certificate file into the installer.

1. Create a folder named **Configure.**
2. Create a single file, named **adagent.cert** that contains one or more X.509 certificates to be distributed to each installation of the Agent, and place it in the Configure folder.
3. Right-click the **AccessDataAgent** package installer file on the install disc, ([*Drive*]**:\Enterprise\Agents\agent-Mac.dmg**).
4. Select **Show Package Contents** popup menu item.
5. Drag the **Configure** folder from the Package Contents into the folder opened in Step 4 (alongside the **Contents** folder).

Configuring the Port

The **AccessDataAgent** installer allows an Administrator to (optionally) configure the port the Agent will use to communicate with an *Examiner* when installed. This is done by adding a file containing the port number to the **AccessDataAgent** package installer. The following is a set of instructions an Administrator will use to configure

the AccessData Agent package installer. To do so, complete Steps 1-5 under Bundling a Certificate, then continue with Step 1 here. If you do not need to do a custom configuration of the port, skip to Step 6 below.

1. Create a text file named **adagent.port** that contains the port number the Agent is to use; this file is to be distributed to each installation of the Agent.
2. Place the **adagent.port** file into the **Configure** folder (previously created to contain the X.509 certificate).
3. Right-click the **AccessDataAgent** package installer file.
4. Select **Show Package Contents** popup menu item.
5. Ensure that the **Configure** folder is located in the same folder opened in Step 4 (alongside the **Contents** folder).
6. Close the window.

> **Note:** The installer will not run successfully if all of the above steps are not already completed. The folder and file names must be exactly as documented

Additional Configuration Options

The Mac installer now supports the same settings as the Unix installer. Each setting should be added to the **.mpkg** file in a directory called **Configure**.

Enterprise Mac Agent Configuration Options

Option	Result
- adagent.cert	Specifies the certificate file used for communication
- adagent.port	Specifies the port the agent will listen on. The setting should contain nothing more than a number. The default port number is 3999
- adagent.lifetime	Specifies the amount of time before the agent dissolves. Again the file should contain nothing more than a number. Same rules as for the Linux agent about sign and value. The default is 0.
- adagent.connections	Sets the maximum number of concurrent connections allowed by the agent. The file should contain only a number. The default is 10.
- adagent.size	Sets the protected storage area size. The file should contain only the number. The default is 16777216. (16 MB).

Installing the Agent

When the certificate is bundled and the port configuration file is complete and saved, distribute the **AccessDataAgent** package installer to each target computer and run it locally.

Uninstalling the Agent

The AccessData Agent can be uninstalled by double-clicking the uninstall utility located in **/Library/Application Support/AccessData**. You will be required to enter your password; you must have administration rights for the uninstall to complete correctly.

Note: The account must have a password assigned to it.

Chapter 41

Working with Windows Registry Evidence

This appendix contains information about the Windows Registry and what information can be gathered from it for evidence. It includes the following topics:

- Understanding the Windows Registry (page 528)
- Windows XP Registry Quick Find Chart (page 533)

Understanding the Windows Registry

For forensic work, registry files are particularly useful because they can contain important information such as the following:

- Usernames and passwords for programs, email, and Internet sites
- A history of Internet sites accessed, including dates and times
- A record of Internet queries (i.e., searches performed on Internet search engines like Google, Yahoo, etc.)
- Lists of recently accessed files (e.g., documents, images, etc.)
- A list of all programs installed on the system

AccessData Registry Viewer allows you to view the contents of Windows operating system registries. Unlike the standard Windows Registry Editor, which only displays the current system's registry, Registry Viewer lets you examine registry files from any Windows system or user. Registry Viewer also provides access to a registry's protected storage, which contains passwords, usernames, and other information not accessible from within Windows Registry Editor.

The files that make up the registry differ depending on the version of Windows. The tables below list the registry files for each version of Windows, along with their locations and the information they contain.

Windows 9x Registry Files

The following table describes each item on the Windows 9*x* registry files.

Windows 9x Registry Files

system.dat	\Windows	• Protected storage for all users on the system. Protected Storage is an access-restricted area of the registry that stores confidential user information including usernames and passwords for Internet web sites, email Internet passwords for Microsoft Outlook or Outlook Express, and a record of queries (i.e., searches performed on Internet search engines like Google, Yahoo, etc.), including the time and date when they were performed. • Lists installed programs, their settings, and any usernames and passwords associated with them. • Contains the System settings.
user.dat	\Windows If there are multiple user accounts on the system, each user has a user.dat file located in \Windows\profiles\user account	• MRU (Most Recently Used) list of files. MRU Lists maintain a list of files so users can quickly re-access files. Registry Viewer allows you to examine these lists to see what files have been recently used and where they are located. Registry Viewer lists each program's MRU files in order from most recently accessed to least recently accessed. • User preference settings (desktop configuration, etc.).

Windows NT and Windows 2000 Registry Files

The following table describes each item in the Windows NT and Windows 2000 registry files.

Windows NT and Windows 2000 Registry Files

NTUSER.DAT	\Documents and Settings\[*user account*] If there are multiple user accounts on the system, each user has an ntuser.dat file.	• Protected storage for all users on the system. Protected Storage is an access-restricted area of the registry that stores confidential user information including usernames and passwords for Internet web sites, email passwords for Microsoft Outlook or Outlook Express, and a record of Internet queries (i.e., searches performed on Internet search engines like Google, Yahoo, etc.), including the time and date when they were performed. • All installed programs, their settings, and any usernames and passwords associated with them. • User preference settings (desktop configuration, etc.).
default	\Winnt\system32\config	System settings.
SAM	\Winnt\system32\config	User account management and security settings.
SECURITY	\Winnt\system32\config	Security settings.
software	\Winnt\system32\config	All installed programs, their settings, and any usernames and passwords associated with them.
system	\Winnt\system32\config	System settings.

Windows XP Registry Files

The following table describes each item in the Windows XP registry files.

Windows XP Registry Files

NTUSER.DAT	\Documents and Settings\[*user account*] If there are multiple user accounts on the system, each user has an ntuser.dat file.	• Protected storage for all users on the system. Protected Storage is an access-restricted area of the registry that stores confidential user information including usernames and passwords for Internet web sites, email passwords for Microsoft Outlook or Outlook Express, and a record of Internet queries (i.e., searches performed on Internet search engines like Google, Yahoo, etc.), including the time and date when they were performed. • All installed programs, their settings, and any usernames and passwords associated with them. • User preference settings (desktop configuration, etc.)
default	\Winnt\system32\config	System settings.
SAM	\Winnt\system32\config	User account management and security settings.
SECURITY	\Winnt\system32\config	Security settings.
software	\Winnt\system32\config	All installed programs, their settings, and any usernames and passwords associated with them.
system	\Winnt\system32\config	System settings.

The logical registry is organized into the following tree structure:

The top level of the tree is divided into hives. A hive is a discrete body of keys, subkeys, and values that is rooted at the top of the registry hierarchy. On Windows XP systems, the registry hives are as follows:

- HKEY_CLASSES_ROOT (HKCR)
- HKEY_CURRENT_USER (HKCU)
- HKEY_LOCAL_MACHINE (HKLM)
- HKEY_USERS (HKU)
- HKEY_CURRENT_CONFIG (HKCC)
- HKEY_DYN_DATA (HKDD)

HKEY_LOCAL_MACHINE and HKEY_USERS are the root hives. They contain information that is used to create the HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, and HKEY_CURRENT_CONFIG hives.

HKEY_LOCAL_MACHINE is generated at startup from the system.dat file and contains all the configuration information for the local machine. For example, it might have one configuration if the computer is docked, and another if the computer is not docked. Based on the computer state at startup, the information in HKEY_LOCAL_MACHINE is used to generate HKEY_CURRENT_CONFIG and HKEY_CLASSES_ROOT.

HKEY_USERS is generated at startup from the system User.dat files and contains information for every user on the system.

Based on who logs in to the system, the information in HKEY_USERS is used to generate HKEY_CURRENT_USER, HKEY_CURRENT_CONFIG, and HKEY_CLASSES_ROOT.

Keys and sub-keys are used to divide the registry tree into logical units off the root.

When you select a key, Registry Editor displays the key's values; that is, the information associated with that key. Each value has a name and a data type, followed by a representation of the value's data. The data type tells you what kind of data the value contains as well as how it is represented. For example, values of the REG_BINARY type contain raw binary data and are displayed in hexadecimal format.

Possible Data Types

The following table lists the Registry's possible data types.

Registry Data Types

REG_BINARY	Binary Value	Raw binary data. Most hardware component information is stored as binary data and is displayed in hexadecimal format.
REG_DWORD	DWORD Value	Data represented by a number that is 4 bytes long (a 32-bit integer). Many parameters for device drivers and services are this type and are displayed in binary, hexadecimal, or decimal format. Related values are REG_DWORD_LITTLE_ENDIAN (least significant byte is at the lowest address) and REG_DWORD_BIG_ENDIAN (least significant byte is at the highest address).
REG_EXPAND_SZ	Expandable String Value	A variable-length data string. This data type includes variables that are resolved when a program or service uses the data.
REG_MULTI_SZ	Multi-String Value	A multiple string. Values that contain lists or multiple values in a format that people can read are usually this type. Entries are separated by spaces, commas, or other marks.
REG_SZ	String Value	A text string of any length.
REG_RESOURCE_LIST	Binary Value	A series of nested arrays designed to store a resource list used by a hardware device driver or one of the physical devices it controls. This data is detected by the system and is displayed in hexadecimal format as a Binary Value.
REG_RESOURCE_REQUIREMENTS_LIST	Binary Value	A series of nested arrays designed to store a device driver's list of possible hardware resources that it, or one of the physical devices it controls, can use. This data is detected by the system and is displayed in hexadecimal format as a Binary Value.
REG_FULL_RESOURCE_DESCRIPTOR	Binary Value	A series of nested arrays deigned to store a resource list used by a physical hardware device. This data is displayed in hexadecimal format as a Binary Value.
REG_NONE	None	Data with no particular type. This data is written to the registry by the system or applications and is displayed in hexadecimal format as a Binary Value.
REG_LINK	Link	A Unicode string naming a symbolic link.
REG_QWORD	QWORD Value	Data represented by a number that is a 64-bit integer.

Additional Considerations

If there are multiple users on a single machine, you must be aware of the following issues when conducting a forensic investigation:

- If there are individual profiles for each user on the system, you need to locate the USER.DAT file for the suspects.
- If all the users on the system are using the same profile, everyone's information is stored in the same USER.DAT file. Therefore, you will have to find other corroborating evidence because you cannot associate evidence in the USER.DAT file with a specific user profile.
- On Windows *9x* systems, the USER.DAT file for the default user is used to create the USER.DAT files for new user profiles. Consequently, the USER.DAT files for new profiles can inherit a lot of junk.

To access the Windows registry from an image of the suspect's drive, you can do any of the following:

- Load the suspect's drive image and export his or her registry files to view them in Registry Editor.
- Mount a restored image as a drive, launch Registry Editor at the command line from your processing machine, export the registry files from the restored image, then view them in a third-party tool.

Note: The problem with this method is that you can only view the registry as text. Registry Editor displays everything in ASCII so you can't see hex or binary values in the registry.

- Use Registry Viewer. Registry Viewer integrates seamlessly with the *Examiner* to display registry files within the image and create reports.

Important: Registry Viewer shows everything you normally see in live systems using the Windows Registry Editor. However, unlike Registry Editor and other tools that use the Windows API, Registry Viewer decrypts protected storage information so it displays values in the Protected Storage System Provider key (PSSP). Registry Viewer also shows information that is normally hidden in null-terminated keys.

Seizing Windows Systems

Information stored in the registry— Internet Messenger sessions, Microsoft Office MRU lists, usernames and passwords for internet Web sites accessed through Internet Explorer, and so forth—are temporarily stored in HKEY_CURRENT_USER. When the user closes an application or logs out, the hive's cached information is pulled out of memory and written to the user's corresponding USER.DAT.

Note: Passwords and MRU lists are not saved unless these options are enabled.

Important: Because normal seizure procedures require that there be no alteration of the suspect's computer in any way, you must be able to articulate why you closed any active applications before pulling the plug on the suspect's computer. Sometimes it is better to simply pull the plug on the computer; other times, it makes more sense to image the computer in place while it is on. It may depend on what is the most important type of data expected to be found on the computer.

For example, Windows updates some program information in the registry when the changes are made. Other information is not updated until a program is closed. Also, if the computer's drive is encrypted and you cannot decrypt it or don't have the Key or password, you may have no choice except to image the live drive.

The Registry Quick Find Chart shown below gives more information.

Windows XP Registry Quick Find Chart

The following charts describe common locations where you can find data of forensic interest in the Windows Registry.

System Information

Windows XP Registry System Information

Registered Owner	Software	Microsoft\Windows NT\CurrentVersion	This information is entered during installation, but can be modified later.
Registered Organization	Software	Microsoft\Windows NT\CurrentVersion	This information is entered during installation, but can be modified later.
Run	Software	Microsoft\Windows\Current Version\Run	Programs that appear in this key run automatically when the system boots.
Logon Banner Message	Software	Microsoft\Windows\Current Version\Policies\System\Legal NoticeText	This is a banner that users must click through to log on to a system.
Mounted Devices	System	MountedDevices	Database of current and prior mounted devices that received a drive letter.
Current Control Set	System	Select	Identifies which control set is current.
Shutdown Time	System	ControlSetXXX\Control\Windows	System shutdown time.
Event Logs	System	ControlSetXXX\Services\Eventlog	Location of Event logs.
Dynamic Disk	System	ControlSetXXX\Services\DMIO\Boot Info\Primary Disk Group	Identifies the most recent dynamic disk mounted in the system.
Pagefile	System	ControlSetXXX\Control\Session Manager\Memory Management	Location, size, set to wipe, etc.
Last User Logged In	Software	Microsoft\Windows NT\CurrentVersion\Winlogon	Last user logged in - can be a local or domain account.
Product ID	Software	Microsoft\Windows NT\CurrentVersion	
O\S Version	Software	Microsoft\Windows NT\CurrentVersion	
Logon Banner Title	Software	Microsoft\Windows\Current Version\Policies\System\Legal NoticeCaption	User-defined data.
Logon Banner Message	Software	Microsoft\Windows\Current Version\Policies\System\Legal NoticeCaption	User-defined data.
Time Zone	System	ControlSet001(or002)\Control\TimeZoneInformation\Standard Name	This information is entered during installation, but can be modified later.

Networking

Windows XP Registry Networking Information

Map Network Drive MRU	NTUSER.DAT	Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU	Most recently used list of mapped network drives.
TCP\IP data	System	ControlSetXXX\Services\TCPIP\Parameters	Domain, hostname data.
TCP\IP Settings of a Network Adapter	System	ControlSetXXX\Services\adapter\Parameters\TCPIP	IP address, gateway information.
Default Printer	NTUSER.DAT	Software\Microsoft\Windows NT\CurrentVersion\Windows	Current default printer.
Default Printer	NTUSER.DAT	\printers	Current default printer.
Local Users	SAM	Domains\Account\Users\Names	Local account security identifiers.
Local Groups	SAM	Domains\Builtin\Aliases\Names	Local account security identifiers.
Profile list	Software	Microsoft\Windows NT\CurrentVersion\ProfileList	Contains user security identifiers (only users with profile on the system).
Network Map	NTUSER.DAT	Documents and Settings\username	Browser history and last-viewed lists attributed to the user.

User Data

Windows XP Registry User Data

Run	NTUSER.DAT	Software\Microsoft\Windows\CurrentVersion\Run	Programs that appear in this key run automatically when the user logs on.
Media Player Recent List	NTUSER.DAT	Software\Microsoft\Media Player\Player\ RecentFileList	This key contains the user's most recently used list for Windows Media Player.
O\S Recent Docs	NTUSER.DAT	Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	MRU list pointing to shortcuts located in the recent directory.
Run MRU	NTUSER.DAT	\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU	MRU list of commands entered in the “run” box.
Open And Save As Dialog Boxes MRU	NTUSER.DAT	\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32	MRU lists of programs\files opened with or saved with the “open” or “save as” dialog boxes.
Current Theme	NTUSER.DAT	Software\Microsoft\Windows\CurrentVersion\Themes	Desktop theme\wallpaper.

Windows XP Registry User Data (Continued)

Last Theme	NTUSER.DAT	Software\Microsoft\Windows\CurrentVersion\Themes\Last Theme	Desktop theme\wallpaper.
File Extensions\ Program Association	NTUSER.DAT	Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts	Identifies associated programs with file extensions.

User Application Data

Windows XP Registry User Application Data

Word User Info	NTUSER.DAT	Software\Microsoft\office\ version\Common\UserInfo	This information is entered during installation, but can be modified later.
Word Recent Docs	NTUSER.DAT	Software\Microsoft\office\ version\Common\Data	Microsoft word recent documents.
IE Typed URLs	NTUSER.DAT	Software\Microsoft\ Explorer\TypedURLs	Data entered into the URL address bar.
IE Auto- Complete Passwords	NTUSER.DAT	\Software\Microsoft\Internet Internet Explorer\IntelliForms	Web page auto complete password-encrypted values.
IE Auto-Complete Web Addresses	NTUSER.DAT	\Software\Microsoft\Protected Storage System Provider	Lists Web pages where auto complete was used.
IE Default Download Directory	NTUSER.DAT	Software\Microsoft\Internet Explorer	Default download directory when utilizing Internet Explorer.
Outlook Temporary Attachment Directory	NTUSER.DAT	Software\Microsoft\office\ version\Outlook\Security	Location where attachments are stored when opened from Outlook.
AIM	NTUSER.DAT	Software\America Online\AOL Instant Messenger\ CurrentVersion\Users\username	IM contacts, file transfer information, etc.
Word User Info	NTUSER.DAT	Software\Microsoft\office\ version\Common\UserInfo	This information is entered during installation, but can be modified later.
ICQ	NTUSER.DAT	\Software\Mirabilis\ICQ*	IM contacts, file transfer information, etc.
MSN Messenger	NTUSER.DAT	Software\Microsoft\MSN Messenger\ListCache\.NET MessngerService*	IM contacts, file transfer information, etc.
Kazaa	NTUSER.DAT	Software\Kazaa*	Configuration, search, download, IM data, etc.
Yahoo	NTUSER.DAT	Software\Yahoo\Pager\ Profiles*	IM contacts, file transfer information, etc.
Google Client History	NTUSER.DAT	Software\Google\NavClient\ 1.1\History	
Adobe	NTUSER.DAT	Software\Adobe*	Acrobat, Photo deluxe, etc.

Chapter 42

Supported File Systems and Drive Image Formats

This appendix lists the file systems and image formats that are analyzed. It includes the following topics:

- File Systems (page 537)
- Whole Disk Encrypted Products (page 538)
- Hard Disk Image Formats (page 538)
- CD and DVD Image Formats (page 539)

File Systems

The following table lists AccessData identified and analyzed file systems.

Identified and Analyzed File Systems	
• FAT 12, FAT 16, FAT 32	• NTFS
• Ext2FS	• HFS, HFS+
• Ext3FS	• CDFS
• Ext4FS	• exFAT
• ReiserFS 3	• Windows 8 and Server 2012 ReFS
• VxFS (Veritas File System)	• Windows 10

Whole Disk Encrypted Products

The following table lists identified and analyzed Whole Disk Encryption (WDE) decryption products (these all require the investigator to enter the password, AccessData forensic products don't "crack" these).

Recognized and Analyzed Whole Disk Encryption Formats

• AFF (Advanced Forensic Format)	• Utimaco Safeguard Easy
• PGP®	• Utimaco SafeGuard Enterprise
• Credant	• Guardian Edge
• SafeBoot	• EFS
• JFS	• LVM
• VMWare	• LVM2
• UFS1	• UFS2
• Apple FileVault	• Apple FileVault 2

Hard Disk Image Formats

The following table lists identified and analyzed hard disk image formats.

Supported Hard Disk Image Formats

• Encase, including 'incomplete' Tableau-created files	• SnapBack
• Safeback 2.0 and under	• Expert Witness
• Linux DD	• ICS
• Ghost (forensic images only)	• SMART
• AccessData Logical Image (AD1)	• MSVHD (MS Virtual Hard Disk)
• DMG (Mac)	• Lx0, Lx01

CD and DVD Image Formats

The following table lists identified and analyzed CD and DVD image formats.

Identified and Analyzed CD and DVD File Systems and Formats

• Alcohol (*.mds)	• IsoBuster CUE
• PlexTools (*.pxi)	• CloneCD (*.ccd)
• Nero (*.nrg)	• Roxio (*.cif)
• ISO	• Pinnacle (*.pdi)
• Virtual CD (*.vc4)	• CD-RW,
• VCD	• CD-ROM
• DVD+MRW	• DVCD
• DVD-RW	• DVD-VFR
• DVD+RW Dual Layer	• DVD-VR
• BD-R SRM-POW	• BD-R
• BD-R SRM	• BD-R DL
• HD DVD-R	• HD DVD-RW DL
• SVCD	• HD DVD
• HD DVD-RW	• DVD-RAM,
• CD-ROM XA	• CD-MRW,
• DVD+VR	• DVD+R
• DVD+R Dual Layer	• BD-RE
• DVD-VRW	• BD-ROM
• HD DVD-R DL	• BD-R RRM
• BDAV	• Virtual CD (*.vc4)
• HD DVD-RAM	• DVD+RW
• CD-R	• VD-R
• SACD	• DVD-R Dual Layer
• DVD-ROM	• BD-R SRM+POW
• DVD-VM	• BD-RE DL
• DVD+VRW	•

Chapter 43
Recovering Deleted Material

You can find deleted files on supported file systems by their file header.

This appendix includes the following topics:

- FAT 12, 16, and 32 (page 540)
- NTFS (page 541)
- Ext2 (page 541)
- Ext3 (page 541)
- HFS (page 541)

FAT 12, 16, and 32

When parsing FAT directories, deleted files are identified by their names. In a deleted file, the first character of the 8.3 filename is replaced by the hex character 0xE5.

The file's directory entry provides the file's starting cluster (C) and size. From the size of the file and the starting cluster, the total number of clusters (N) occupied by the file are computed.

The File Allocation Table (FAT) is examined and the number of unallocated clusters are counted, starting at C (U). The recovered file [min (N, U)] clusters starting at C are then assigned.

If the deleted file was fragmented, the recovered file is likely to be incorrect and incomplete because the information that is needed to find subsequent fragments was wiped from the FAT system when the file was deleted.

If present, the long filename (LFN) entries are used to recover the first letter of the deleted file's short filename. If the LFN entries are incomplete or absent, it uses an exclamation mark ("!") as the first letter of the filename.

The volume free space for deleted directories that have been orphaned are searched with a meta-carve process. An orphaned directory is a directory whose parent directory or whose entry in its parent directory has been overwritten.

NTFS

The Master File Table (MFT) is examined to find files that are marked deleted because the allocation byte in a record header indicates a deleted file or folder. It then recovers the file's data using the MFT record's data attribute extent list if the data is non-resident.

If the deleted file's parent directory exists, the recovered file is shown in the directory where it originally existed. Deleted files whose parent directories were deleted are shown in their proper place as long as their parent directory's MFT entry has not been recycled.

Ext2

Nodes that are marked deleted are searched for. The link count is zero and the deletion timestamp is nonzero.

For each deleted inode, the block pointers are processed and blocks are added to the deleted file. However, if an indirect block is marked allocated or references an invalid block number, the recovered file is truncated at that point because the block no longer contains a list of blocks for the file that the application is attempting to recover.

The filenames for files deleted on ext2 systems are not recovered. Instead, deleted files are identified by inode number because ext2 uses variable-length directory entries organized in a linked list structure. When a file is deleted, its directory entry is unlinked from the list, and the space it occupied becomes free to be partially or completely overwritten by new directory entries. There is no reliable way to identify and extract completely deleted directory entries.

Ext3

Deleted files from ext3 volumes are not recovered because ext3 zeroes out a file's indirect block pointers when it is deleted.

HFS

Deleted files from HFS are not recovered.

Chapter 44

Managing Security Devices and Licenses

This appendix includes information AccessData product licenses, Virtual CodeMeter activation, and Network License Server configurations.

Installing and Managing Security Devices

AccessData products require a licensing security device that communicates with the program to verify the existence of a current license.

You must install the security device software and drivers before you can manage licenses with LicenseManager. This section explains installing and using the CodeMeter Runtime software and the License Manager.

Installing the Security Device

AccessData products require a licensing security device that communicates with the program to verify the existence of a current license. The device is a WIBU-SYSTEMS (Wibu) CodeMeter (CmStick). This USB device requires specific software to be installed prior to connecting the devices and running your AccessData products. You will need the WIBU-SYSTEMS CodeMeter Runtime software with a WIBU-SYSTEMS CodeMeter (CmStick), either the physical USB device, or the Virtual device.

Store the CmStick or dongle in a secure location when it is not in use.

Installing the CodeMeter Runtime Software

When you purchase a product, AccessData provides a USB CmStick with the product package. To use the CmStick, you must first install the CodeMeter Runtime software, either from the shipping disc or from the setup file downloaded from the AccessData Web site.

Note: The CodeMeter software is automatically installed as part of the FTK suite.

To download the CodeMeter installer from the AccessData web site

1. Go to the AccessData download page at: http://www.accessdata.com/product-download.
2. On the download page, click **CodeMeter**.
3. Click **Download Page**.

4. Click **Download Now**.
5. Save the installation file to your download directory or other temporary directory on your drive.

To install CodeMeter

1. Do one of the following:
   - Launch the installer from the FTK installer by doing the following:
     1a. Launch the FTK installer **Autorun.exe** file.
     1b. Click **Other Products**.
     1c. Click Install License Manager.
   - Launch the installer from the download by doing the following:
     1a. Navigate to, and double-click the installation file.
2. Wait for the *Preparing to Install* processes to complete.
3. In the Welcome dialog, click **Next**.
4. Read and accept the License Agreement
5. Enter User Information.
6. Click **Next**.
7. Select the features you want to install.
8. Click **Next**.
9. Click **Install**.
10. Click **Finish**.
11. Click **OK**.

CodeMeter Error

If you are not using NLS for your security device configuration, after clicking **No,** you will see the following additional message.

Security Device Not Found

To remedy, click **OK**, then install the correct CodeMeter Runtime software, and connect the CmStick or run License Manager to generate your Virtual CmStick. Then, restart FTK.

Installing LicenseManager

LicenseManager lets you manage product and license subscriptions using a security device or device packet file.

You can can access the LicenseManager installer from the Web or from the FTK installer.

To download the LicenseManager installer from the AccessData web site

1. Go to the AccessData download page at: http://www.accessdata.com/product-download.
2. On the download page, click **LicenseManager**.
3. Click **Download Page**.
4. Click **Download Now**.
5. Save the installation file to your download directory or other temporary directory on your drive.

To install LicenseManager

1. Do one of the following:
   - Launch the installer from the FTK installer by doing the following:
     1a. Launch the FTK installer **Autorun.exe** file.
     1b. Click **Other Products**.
     1c. Click Install License Manager.
   - Launch the installer from the download by doing the following:
     1a. Navigate to, and double-click the installation file.
2. Wait for the *Preparing to Install* processes to complete.
3. Click **Next** on the Welcome screen
4. Read and accept the License Agreement.
5. Click **Next**.
6. Accept the default destination folder, or select a different one.
7. Click **Next**.
8. In the Ready to Install the Program dialog, click **Back** to review or change any of the installation settings. When you are ready to continue, click **Install**.
9. Wait while the installation completes.
10. If you want to launch LicenseManager after completing the installation, mark the **Launch AccessData LicenseManager** check box.
11. Select the **Launch AccessData LicenseManager** check box to run the program upon finishing the setup. The next section describes how to run LicenseManager later.
12. Click **Finish** to finalize the installation and close the wizard.

Starting LicenseManager

To launch LicenseManager

1. Launch LicenseManager by clicking the **LicenseManager** icon on your desktop.

   When starting, LicenseManager reads licensing and subscription information from the installed and connected WIBU-SYSTEMS CodeMeter Stick, or Keylok dongle.

   Note: If using a Keylok dongle, and LicenseManager either does not open or displays the message, "Device Not Found"

2. Verify the correct dongle driver is installed on your computer.
3. With the dongle connected, check in Windows Device Manager to make sure the device is recognized. If it has an error indicator, right click on the device and choose Uninstall.
4. Remove the dongle after the device has been uninstalled.
5. Reboot your computer.
6. After the reboot is complete, and all startup processes have finished running, connect the dongle.
7. Wait for Windows to run the Add New Hardware wizard. If you already have the right dongle drivers installed, do not browse the internet, choose, "No, not this time."
8. Click **Next** to continue.
9. On the next options screen, choose, "Install the software automatically (Recommended)
10. Click **Next** to continue.
11. When the installation of the dongle device is complete, click Finish to close the wizard.
12. You still need the CodeMeter software installed, but will not need a CodeMeter Stick to run LicenseManager.

    Note: If using a CodeMeter Stick, and LicenseManager either does not open or displays the message, "Device Not Found"

13. Make sure the CodeMeter Runtime 4.20b software is installed. It is available at **www.accessdata.com/support**. Click Downloads and browse to the product. Click on the download link. You can **Run** the product from the Website, or **Save** the file locally and run it from your PC. Once the CodeMeter Runtime software is installed and running, you will see a gray icon in your system tray.
14. Make sure the CodeMeter Stick is connected to the USB port.

If the CodeMeter Stick is not connected, LicenseManager still lets you to manage licenses using a security device packet file if you have exported and saved the file previously.

To open LicenseManager without a CodeMeter Stick installed

1. Click **Tools** > **LicenseManager**.

   LicenseManager displays the message, "Device not Found".

2. Click **OK**, then browse for a security device packet file to open.

Note: Although you can run LicenseManager using a packet file, AccessData products will not run with a packet file alone. You must have the CmStick or dongle connected to the computer to run AccessData products that require a license.

Using LicenseManager

LicenseManager provides the tools necessary for managing AccessData product licenses on a WIBU-SYSTEMS CodeMeter Stick security device, a Keylok dongle, a Virtual Dongle, or in a security device packet file.

LicenseManager displays license information, allows you to add licenses to or remove existing licenses from a dongle or CmStick. LicenseManager, and can also be used to export a security device packet file. Packet files can be saved and reloaded into LicenseManager, or sent via email to AccessData support.

In addition, you can use LicenseManager to check for product updates and in some cases download the latest product versions.

LicenseManager displays CodeMeter Stick information (including packet version and serial number) and licensing information for all AccessData products. The Purchase Licenses button connects directly to the AccessData website and allows you to browse the site for information about products you may wish to purchase. Contact AccessData by phone to speak with a Sales Representative for answers to product questions, and to purchase products and renew licenses and subscriptions.

The LicenseManager Interface

The LicenseManager interface consists of two tabs that organize the options in the LicenseManager window: the Installed Components tab and the Licenses tab.

The Installed Components Tab

The Installed Components tab lists the AccessData programs installed on the machine. The Installed Components tab is displayed in the following figure.

The following information is displayed on the Installed Components tab:

LicenseManager Installed Components Tab Features

Program	Lists all AccessData products installed on the host.
Installed Version	Displays the version of each AccessData product installed on the host.
Newest Version	Displays the latest version available of each AccessData product installed on the host. Click **Newest** to refresh this list.
Product Notes	Displays notes and information about the product selected in the program list.
AccessData Link	Links to the AccessData product page where you can learn more about AccessData products.

The following buttons provide additional functionality from the Installed Components tab:

LicenseManager Installed Components Buttons

Help	Opens the LicenseManager Help web page.

LicenseManager Installed Components Buttons (Continued)

Install Newest	Installs the newest version of the programs checked in the product window, if that program is available for download. You can also get the latest versions from our website using your Internet browser.
Newest	Updates the latest version information for your installed products.
About	Displays the About LicenseManager screen. Provides version, copyright, and trademark information for LicenseManager.
Done	Closes LicenseManager.

Use the Installed Components tab to manage your AccessData products and stay up to date on new releases.

The Licenses Tab

The Licenses tab displays CodeMeter Stick information for the current security device packet file and licensing information for AccessData products available to the owner of the CodeMeter Stick, as displayed in the following figure.

The Licenses tab provides the following information:

LicenseManager Licenses Tab Features

Program	Shows the owned licenses for AccessData products.
Expiration Date	Shows the date on which your current license expires.
Status	Shows these status of that product's license: ● **None**: the product license is not currently owned ● **Days Left**: displays when less than 31 days remain on the license. ● **Never**: the license is permanently owned. This generally applies to Hash Tables and Portable Office Rainbow Tables.
Name	Shows the name of additional parameters or information a product requires for its license.
Value	Shows the values of additional parameters or information a product contained in or required for its license.
Show Unlicensed	When checked, the License window displays all products, whether licensed or not.

The following license management actions can be performed using buttons found on the License tab:

License Management Options

Remove License	Removes a selected license from the Licenses window and from the CodeMeter Stick or dongle. Opens the AccessData License Server web page to confirm success.
Refresh Device	Connects to the AccessData License Server. Downloads and overwrites the info on the CodeMeter Stick or dongle with the latest information on the server.
Reload from Device	Begins or restarts the service to read the licenses stored on the CodeMeter Stick or dongle.

License Management Options (Continued)

Release Device	Click to stop the program reading the dongle attached to your machine, much like Windows' Safely Remove Hardware feature. Click this button before removing a dongle. This option is disabled for the CodeMeter Stick.
Open Packet File	Opens Windows Explorer, allowing you to navigate to a .PKT file containing your license information.
Save to File	Opens Windows Explorer, allowing you to save a .PKT file containing your license information. The default location is My Documents.
Finalize Removal	Finishes the removal of licenses in the unbound state. Licenses must be unbound from the CmStick or dongle before this button takes effect.
View Registration Info	Displays an HTML page with your CodeMeter Stick number and other license information.
Add Existing License	Allows you to bind an existing unbound license to your CodeMeter Stick, through an internet connection to the AccessData License Server.
Purchase License	Brings up the AccessData product page from which you can learn more about AccessData products.
About	Displays the About LicenseManager screen. Provides version, copyright, and trademark information for LicenseManager.
Done	Closes LicenseManager.

Opening and Saving Dongle Packet Files

You can open or save dongle packet files using LicenseManager. When started, LicenseManager attempts to read licensing and subscription information from the dongle. If you do not have a dongle installed, LicenseManager lets you browse to open a dongle packet file. You must have already created and saved a dongle packet file to be able to browse to and open it.

To save a security device packet file

1. Click the **Licenses** tab, then under License Packets, click **Save to File**.
2. Browse to the desired folder and accept the default name of the .PKT file; then click **Save**.

> **Note:** In general, the best place to save the .PKT files is in the AccessData LicenseManager folder. The default path is C:\Program Files\AccessData\Common Files\AccessData LicenseManager\.

To open a security device packet file

1. Select the **Licenses** tab.
2. Under License Packets, click **Open Packet File**.
3. Browse for a dongle packet file to open. Select the file and click **Open**.

Adding and Removing Product Licenses

On a computer with an Internet connection, LicenseManager lets you add available product licenses to, or remove them from, a dongle.

To move a product license from one dongle to another dongle, first remove the product license from the first dongle. You must release that dongle, and connect the second dongle before continuing. When the second dongle is connected and recognized by Windows and LicenseManager, click on the Licenses tab to add the product license to the second dongle.

Removing a License

To remove (unassociate, or unbind) a product license

1. From the Licenses tab, mark the program license to remove.

   This action activates the Remove License button below the Program list box.
2. Click **Remove License** to connect your machine to the AccessData License Server through the internet.
3. When you are prompted to confirm the removal of the selected licenses from the device, click **Yes** to continue, or **No** to cancel.
4. Several screens appear indicating the connection and activity on the License Server, and when the license removal is complete, the following screen appears.
5. Click **OK** to close the message box.

   Another internet browser screen appears from LicenseManager with a message that says, “The removal of your licenses from Security Device was successful!” You may close this box at any time.

Adding a License

To add a new or released license

1. From the Licenses tab, under Browser Options, click **Add Existing License.**

   The AccessData LicenseManager Web page opens, listing the licenses currently bound to the connected security device, and below that list, you will see the licenses that currently are not bound to any security device. Mark the box in the Bind column for the product you wish to add to the connected device, then click **Submit**.
2. An AccessData LicenseManager Web page will open, displaying the following message, “The AccessData products that you selected has been bound to the record for Security Device *nnnnnnn* within the Security Device Database.

   “Please run LicenseManager’s “Refresh Device” feature in order to complete the process of binding these product licenses to this Security Device.” You may close this window at any time.
3. Click **Yes** if LicenseManager prompts, “Were you able to associate a new product with this device?”
4. Click **Refresh Device** in the Licenses tab of LicenseManager. Click **Yes** when prompted.

You will see the newly added license in the License Options list.

Adding and Removing Product Licenses Remotely

While LicenseManager requires an Internet connection to use some features, you can add or remove licenses from a dongle packet file for a dongle that resides on a computer, such as a forensic lab computer, that does not have an Internet connection.

If you cannot connect to the Internet, the easiest way to move licenses from one dongle to another is to physically move the dongle to a computer with an Internet connection, add or remove product licenses as necessary using LicenseManager, and then physically move the dongle back to the original computer. However,

if you cannot move the dongle—due to organization policies or a need for forensic soundness—then transfer the packet files and update files remotely.

Adding a License Remotely

To remotely add (associate or bind) a product license

1. On the computer where the security device resides:
   1a. Run LicenseManager.
   1b. From the **Licenses** tab, click **Reload from Device** to read the dongle license information.
   1c. Click **Save to File** to save the dongle packet file to the local machine.
2. Copy the dongle packet file to a computer with an Internet connection.
3. On the computer with an Internet connection:
   3a. Remove any attached security device.
   3b. Launch LicenseManager. You will see a notification, “No security device found”.
   3c. Click OK.
   3d. An “Open” dialog box will display. Highlight the **.**PKT file, and click **Open**.
   3e. Click on the **Licenses** tab.
   3f. Click **Add Existing License.**
   3g. Complete the process to add a product license on the Website page.
   3h. Click **Yes** when the LicenseManager prompts, “Were you able to associate a new product with this dongle?”
   3i. When LicenseManager does not detect a dongle or the serial number of the dongle does not match the serial number in the dongle packet file, you are prompted to save the update file, **[serial#].wibuCmRaU.**
   3j. Save the update file to the local machine.
4. After the update file is downloaded, copy the update file to the computer where the dongle resides:
5. On the computer where the dongle resides:
   5a. Run the update file by double-clicking it. (**[serial#].wibuCmRaU** is an executable file.)
   5b. After an update file downloads and installs, click **OK.**
   5c. Run LicenseManager.
   5d. From the Licenses tab, click **Reload from Device** to verify the product license has been added to the dongle.

Removing a License Remotely

To remotely remove (unassociate, or unbind) a product license

1. On the computer where the dongle resides:
   1a. Run LicenseManager.
   1b. From the Licenses tab, click **Reload from Device** to read the dongle license information.
   1c. Click **Save to File** to save the dongle packet file to the local machine.
2. Copy the file to a computer with an Internet connection.
3. On the computer with an Internet connection:
   3a. Launch LicenseManager. You will see a notification, “No security device found”.

3b. Click **OK**.

3c. An “Open” dialog box will display. Highlight the **.**PKT file, and click **Open**.

3d. Click on the Licenses tab.

3e. Mark the box for the product license you want to unassociate; then click **Remove License.**

3f. When prompted to confirm the removal of the selected license from the dongle, click **Yes**.

3g. When LicenseManager does not detect a dongle or the serial number of the dongle does not match the serial number in the dongle packet file, you are prompted save the update file.

3h. Click **Yes** to save the update file to the local computer.

3i. The Step 1 of 2 dialog details how to use the dongle packet file to remove the license from a dongle on another computer.

3j. Save the update file to the local machine.

4. After the update file is downloaded, copy the update file to the computer where the dongle resides.
5. On the computer where the dongle resides:

5a. Run the update file by double-clicking it. This runs the executable update file and copies the new information to the security device.

5b. Run LicenseManager

5c. On the Licenses tab, click **Reload from Device** in LicenseManager to read the security device and allow you to verify the product license is removed from the dongle.

5d. Click **Save to File** to save the updated dongle packet file to the local machine.

6. Copy the file to a computer with an Internet connection.

Updating Products

You can use LicenseManager to check for product updates and download the latest product versions.

Checking for Product Updates

To check for product updates, on the Installed Components tab, click **Newest**. This refreshes the list to display what version you have installed, and the newest version available.

Downloading Product Updates

To install the newest version, mark the box next to the product to install, then click **Install Newest**.

Note: Some products are too large to download, and are not available. A notification displays if this is the case.

To download a product update

1. Ensure that LicenseManager displays the latest product information by clicking the Installed Components tab. Click **Newest** to refresh the list showing the latest releases, then compare your installed version to the latest release.

   If the latest release is newer than your installed version, you may be able to install the latest release from our Website.
2. Ensure that the program you want to install is not running.
3. Mark the box next to the program you want to download; then click **Install Newest**.

4. When prompted, click **Yes** to download the latest install version of the product.
   4a. If installing the update on a remote computer, copy the product update file to another computer.
5. Install the product update. You may need to restart your computer after the update is installed.

Purchasing Product Licenses

Use LicenseManager to link to the AccessData Web site to find information about all our products.

Purchase product licenses through your AccessData Sales Representative. Call 801-377-5410 and follow the prompt for Sales, or send an email to sales@accessdata.com.

Note: Once a product has been purchased and appears in the AccessData License Server, add the product license to a CodeMeter Stick, dongle, or security device packet file by clicking **Refresh Device**.

Sending a Dongle Packet File to Support

Send a security device packet file **only** when specifically directed to do so by AccessData support.

To create a dongle packet file

1. Run LicenseManager
2. Click on the Licenses tab.
3. Click **Load from Device**.
4. Click **Refresh Device** if you need to get the latest info from AD's license server.
5. Click **Save to File**, and note or specify the location for the saved file.
6. Attach the dongle packet file to an e-mail and send it to: **support@accessdata.com**.

Virtual CodeMeter Activation Guide

Introduction

A Virtual CodeMeter (VCM) allows the user to run licensed AccessData products without a physical CodeMeter device. A VCM can be created using AccessData License Manager, but requires the user to enter a Confirmation Code during the creation process.

The latest revision of this guide can be found at:

http://accessdata.com/downloads/media/VCM_Activation_Guide.pdf

Preparation

- Contact your AccessData sales rep to order a VCM confirmation code.
- Install CodeMeter Runtime 4.10b or newer (available on the AccessData download page).
- Install the latest release of License Manager (available on the AccessData download page).
- The following steps are to be run on the system where you want to permanently attach the VCM.

Note: Once created, the VCM cannot be moved to any other system.

- AD Lab WebUI and eDiscovery administrators, please also follow steps outlined under in Additional Instructions for AD Lab WebUI and eDiscovery (page 555) in order to enable VCM licensing on the AccessData License Service.

Setup for Online Systems

To setup a Virtual CodeMeter

1. Unplug any AccessData dongles you currently have connected.
2. Launch License Manager.

Note: When creating a VCM on Windows Server 2003 or 2008, please refer to the special set of steps written for those platforms. See Creating a Virtual CM-Stick with Server 2003/2008 Enterprise Editions (page 554).

3. Select **Create A Local Virtual CMStick**
4. Click **OK.**
   The Confirmation Code Required dialog appears.
5. Enter your confirmation code.
6. Click **OK**, AccessData License Manager will automatically synchronize with the License Server over the Internet.
7. Click **OK** when the update completes. License Manager will then create the VCM on your system.
8. At this point, AccessData License Manager now displays a serial number for the VCM on the Licenses tab and the VCM can now operate in a similar way to a hardware CodeMeter device.

Setting up VCM for Offline Systems

You can setup a Virtual CodeMeter on a system that is not connected to the internet (offline). You must also have one machine that connects to the internet to perform certain steps. This section details what to do on which machine.

Perform these steps on the Online system

1. Unplug any AccessData dongles you currently have connected.
2. Launch License Manager.

> **Note:** When creating a VCM on Windows Server 2003 or 2008 Enterprise Edition, please refer to the special set of steps written for those platforms. See Creating a Virtual CM-Stick with Server 2003/2008 Enterprise Editions (page 554).

3. Select **Create Empty Virtual CMStick (offline)**.
4. Click **OK.**
5. The resulting dialog prompts you to save the ***.wibucmrau** file. Enter a name and path for the file, then click **Save**.
6. Transfer the ***.wibucmrau** to the Online system.

Perform these steps on the Online system

7. Unplug any AccessData dongles you currently have connected.
8. Launch License Manager.
9. Select **Create Activation File (online)**.
10. Click **OK**.
11. In the Confirmation Code Required dialog, enter your confirmation code and click **OK**.
12. AccessData License Manager will automatically synchronize with the License Server over the internet. Data synchronized from the server will be written to the ***.wibucmrau** file. Click **OK** when the update completes.
13. Transfer ***.wibucmrau** back to the offline system.

Perform these steps on the Offline system

14. Unplug any AccessData dongles you currently have connected.
15. Launch License Manager.
16. Select **Create Activate Virtual CMStick (offline)**.
17. Click **OK**.
18. The resulting dialog prompts you to browse to the location of the newly updated *.**wibucmrau** file. Locate the file, then click **Open**. License Manager creates the VCM on your system.
19. 19.At this point, AccessData License Manager should now display a serial number for the VCM on the “Licenses” tab and the VCM can now operate in a similar way to a hardware CodeMeter device.

Creating a Virtual CM-Stick with Server 2003/2008 Enterprise Editions

This section contains special instructions for using a VCM with Windows Server 2003 or 2008 Enterprise Editions. Complete each section in order.

To Create an Empty CodeMeter License Container

1. On the Server 2003/2008 machine, unplug any CodeMeter devices.
2. Open the CodeMeter Control Center. Make sure the window on the License tab is, empty indicating that no licenses are currently loaded.
3. Select **File > Import License.**
4. Browse to the License Manager program files directory.
   - 32 bit systems: **C:\Program Files\AccessData\LicenseManager**
   - 64 bit systems: **C:\Program Files (x86)\ AccessData\LicenseManager**
5. Highlight the **TemplateDisc5010.wbb** file, then click **Import**.
6. Click the **Activate License** button.
7. When the *CmFAS Assistant* opens, click **Next**.
8. Select **Create license request**, and click **Next**.
9. Confirm the desired directory and filename to save **.WibuCmRaC**. (Example: **Test1.WibuCmRaC**)
10. Click **Commit**.
11. Click **Finish**.

To Copy to another machine

1. Copy the new **.WibuCmRaC** to another machine that is not running Windows Server 2003/2008 Enterprise.

   Note: The destination system must have an active internet connection.

2. Unplug any AccessData dongles you currently have connected.
3. Launch *License Manager*.
4. Select **Create Activation File (online)**.
5. Click **OK**.
6. In the Confirmation Code Required dialog enter your confirmation code and click **OK**.
7. AccessData License Manager will automatically synchronize with the License Server over the internet. Data synchronized from the server will be written to the ***.wibucmrau** file. Click **OK** when the update completes.

To Finish the activation on the Windows Server 2003/2008 Enterprise system

1. Copy the activated **.WibuCmRaC** file to the Server 2003/2008 machine.
2. On the Server 2003/2008 machine, unplug any CodeMeter devices.
3. Open the CodeMeter Control Center. Make sure the window on the License tab empty indicating that no licenses are currently loaded.
4. Select **File > Import License.**
5. Browse to the location where the activated **.WibuCmRaC** is stored. Click **Import**.
6. AccessData License Manager now displays a serial number for the VCM on the Licenses tab and the VCM can now operate in a similar way to a hardware CodeMeter device.

Additional Instructions for AD Lab WebUI and eDiscovery

This section provides additional information for enabling the Web User Interface to recognize a VCM.

To enable AD Lab WebUI and eDiscovery to use VCM

1. Open Registry Editor.
2. Navigate to the following key:

   HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Products

   Add the following DWORD registry string to the key and set the value to 1:

   HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Products | EnableACTTest

The *AccessData License Service* will know to expect a VCM when *EnableACTTest* is set to “1.”

Virtual CodeMeter FAQs

Q: How do I get a Virtual CodeMeter (VCM)?

A: Contact your AccessData product sales representative. They will provide you with a VCM confirmation code.

Q: How do VCMs work?

A: A VCM operates in almost exactly the same way as a hardware CodeMeter device, except that they exist as a file stored on the hard disk. During activation, the VCM file (named with a WBB extension) is tied to the hardware of the system using unique hardware identifiers. Those unique identifiers make VCMs non-portable. When AccessData License Manager is launched, it will automatically load the VCM and display its license information. From there, you can refresh, remove, add existing licenses, etc just the same you would with a hardware security device.

Q: Are VCMs supported on virtual machines (VM)?

A: No. Due to the fact that virtual machines are portable and VCMs are not, VCMs are not supported on virtual machines. Currently it is recommended to use AccessData Network License Service (NLS) to license systems running as virtual machines. CLICK HERE for more information.

Q: Does the AccessData Network License Service (NLS) support VCMs?

A: The current release of NLS does not support using VCM as a network dongle. AccessData is considering this support for a future release.

Q: How can I “unplug” a VCM?

A: If you want to prevent License Manager from automatically loading the VCM you can "unplug" it by stopping the CodeMeter Runtime Service server and then moving (cut and paste) the WBB file to a new location (renaming the file does not suffice). By default the WBB file is located at:

32 bit systems:

C:\Program Files\CodeMeter\CmAct\

64 bit systems:

C:\Program Files (x86)\CodeMeter\CmAct\

Q: I have activated a VCM on my system, but now I need to activate it on a different system. What should I do?

A: Since a VCM is uniquely tied to the system on which it is activated, it cannot be moved to any other system. If you need to activate a VCM on a different system, you need to contact your AccessData Sales Representative.

Q: What if I need to reinstall Windows, format my drive, change my system's hardware, or back up my VCM in case of a disaster? Will the VCM still work?

A: The VCM can be backed up by simply copying the WBB file to a safe location. It can be restored by copying the WBB file to the CmAct folder. The VCM cannot be restored without a WBB file. If you do not have a backup of your WBB file, you will need to get a new confirmation code from your AccessData Sales Representative.

Q: My AccessData product does not seem to recognize the license stored on a VCM. What am I doing wrong?

A: VCMs are supported by the following versions of AccessData products:

- FTK 1.81.6 and newer
- FTK 3.1.0 and newer
- PRTK 6.5.0 and newer
- DNA 3.5.0 and newer
- RV 1.6.0 and newer
- eDiscovery 3.1.2 and newer
- AD Lab 3.1.2 and newer
- AD Enterprise 3.1.0 and newer
- MPE+ 4.0.0.1 and newer

Ensure that the version of the product you are running support VCMs. If the version you are running is listed as supported, verify that according to License Manager, the release date of the version you are running falls before the expiration date of the license.

Network License Server (NLS) Setup Guide

Introduction

This section discusses the installation steps and configuration notes needed to successfully setup an AccessData Network License Server (NLS).

Note: Click on this link to access the latest version of this guide:

Network License Server (NLS) Setup Guide.

Preparation Notes

- CodeMeter Runtime 3.30a or newer must be installed on all Client and Server systems
- AccessData License Manager must be used to prepare the network dongle. The system running License Manager must have internet access and have CodeMeter Runtime installed.
- The current release of NLS supports the following versions of Windows:
  - Windows XP 32/64 bit
  - Windows Server 2003 32/64 bit
  - Windows Vista 32/64 bit
  - Windows Server 2008 R1 32/64 bit
  - Windows 7 32/64 bit
  - Windows Server 2008 R2 64 bit

Setup Overview

To setup NLS

1. Download the latest release of NLS located in the utilities section of the AccessData download page.
2. Extract contents of ZIP to a folder of your choice.
3. On the NLS server system, run through the NLS Installation MSI and accept all defaults.
4. Prepare network dongle:
   4a. Provide the serial number to AD Support and request to have the “Network Dongle Flag” applied.
   4b. Migrate any additional licenses to the network dongle
   4c. Refresh the network dongle device using AccessData License Manager.
5. Launch the AccessData product on the NLS client system.
6. Enter the NLS server configuration information:
   - IP address or hostname of NLS server system
   - Port 6921
7. Click, **OK**.

If you encounter any problems, please read the notes below for troubleshooting information.

Network Dongle Notes

- AccessData License Manager 2.2.6 or newer should be installed in order to manage licenses on the network dongle.
- Network dongles can hold up to 120 physical licenses. Each License has a capacity to hold thousands of sub licenses (i.e. Client count or worker count).
- Contact AccessData Technical Support to have your CodeMeter device flagged as a Network Dongle (required for NLS).

NLS Server System Notes

- Make sure the CodeMeter device is flagged as Network Dongle (i.e. License Manager will show the serial as “1181234N”. To have this flag set on your CodeMeter device, please contact AccessData Technical Support).
- Server system must be configured to allow incoming and outgoing traffic on TCP port 6921.
- A web interface to view and revoke licenses all licenses is accessible at

  `http://localhost:5555`

  This page can be reached only from a web browser running locally on the NLS server system.
- A Network Dongle cannot be used to run AccessData products locally unless the NLS server is running locally.
- Some versions of Windows may not find a local NLS server when the DNS hostname of the server is provided. In those cases, it is recommended to use a static IP address.
- When using the NLS across domains, users must have permissions to access resources on both domains (either by dual-domain membership or cross-domain trust).
- When running NLS on Windows Server 2008, Terminal Services must be installed and accepting connections. If Terminal Services is not configured it will not open the port and share out the licenses correctly.
- The name of the service according to Windows is “AccessData Network License Service.”

NLS Client System Notes

- When launched, any NLS client application that needs to lease a license from the NLS server will automatically check for the following values within the Windows Registry.
  - **NetDonglePath**: The IP address or DNS hostname of the system hosting the Network License Server service which is found in the following registry key on the client system:

    `HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Products\Common`
  - **NetDonglePort**: The TCP port number through which the client and server systems have been configured to use. This value is located in the same key as NetDonglePath.
  - **uniqueId**: In order to lease a license from the server, the client system must first posses a unique identification value. This value is automatically generated by applications such as FTK, PRTK, or DNA. (Registry Viewer and FTK 1.x cannot be used setup initial client NLS configuration at this time.)

    You can find the each client system’s uniqueId by inspecting the following registry key:

    `HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Shared`
- The Client system must be configured to allow all incoming and outgoing traffic on TCP port 6921.
- The following products support the ability to lease a license from a NLS server:
  - FTK 2.2.1 and newer
  - FTK 1.81.2 and newer

    - FTK Pro 3.2 and newer
    - PRTK 6.4.2 and newer
    - DNA 3.4.2 and newer
    - Registry Viewer 1.5.4 and newer
    - AD Enterprise 3.0.3 and newer
    - AD Lab 3.0.4 and newer
    - AD Lab Lite 3.1.2 and previous
    - Mobile Phone Examiner 3.0 and newer
    - Explicit Image Detection (EID) Add-on
    - Glyph Add-on
- Use AccessData License Manager (ver. 2.2.4 or newer) to migrate licenses off other devices and onto a network device.
- When running AccessData products on Windows Vista, 7, or Server 2008 you must choose **Run as administrator** at least once in order to lease a license from a NLS server.
- If the NLS client application is having trouble leasing a license either from the NLS server, AccessData recommends that you reset the licensing configuration to default.
- To reset the licensing configuration, delete and recreate the NLS registry key located at:

  HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Products\Common

Chapter 45

Configuring a Multi-box Setup

Configuration for a Multi-box Setup

A multi-box setup is a configuration where all components are not installed or contained on the same computer. For example, you may have the database installed on a separate computer from the application, or the application and the database are installed on one computer and the case files are stored on a different computer.

By default, a multi-box installation is not configured to allow the user to back up and restore case information. Some configuration changes must be performed manually by the system administrator to properly configure a multi-box installation. Please note that the steps required to complete this configuration differ slightly for domain systems than for workgroup systems.

Configuration Overview

The following steps are required before you can perform multi-box case back ups and restoration.

- Create a service account common to all systems involved. See Create a Service Account on page 561.
- Share the case folder and assign appropriate permissions. See Share the Case Folder on page 562.
- Configure the database services to run under service account. See Configure Database Services on page 563.
- Share back up destination folder with appropriate permissions. See Share the Backup Destination Folder on page 563.

Note: When prompted to select the backup destination folder, *always* use the UNC path of that shared folder, even when the backup destination folder is local.

Each of these items is explained in detail later in this chapter.

Create a Service Account

To function in a distributed configuration, all reading and writing of case data should be performed under the authority of a single Windows user account. Throughout the rest of this document, this account is referred to as the “service account.” If all the systems involved are members of the same domain, choosing a domain user account is the recommended choice. If not all of the systems are members of the same domain, then you can configure “Mirrored Local Accounts” as detailed in the following steps:

To set up Mirrored Local Accounts

1. On the Examiner host system, create (or identify) a local user account.
2. Ensure that the chosen account is a member of the Local Administrators group.
3. On the database host system, create a user that has the exact same username and password as that on the Examiner host system.
4. Ensure that this account is also a member of the Local Administrators group on the database host system.

Instructions for Domain User Accounts

Choose (or create) a domain user account that will function as the service account. Verify that the chosen domain user has local administrator privilege on both the Examiner host system and the database host system.

To verify the domain user account privileges

1. Open the “Local Users and Groups” snap-in.
2. View the members of the Administrators group.
3. Ensure that the account selected earlier is a member of this group (either explicitly or by effective permissions).
4. Perform this verification for both the examination and the database host systems.

Share the Case Folder

On the system hosting the Examiner, create a network share to make the main case folder available to other users on the network. The case folder is no longer assigned by default. The user creating the case creates the case folder. It is that folder that needs to be shared.

For this example, it is located at the root of the Windows system volume, and the pathname is:

C:\FTK-Cases.

To share the case folder

1. Before you can effectively share a folder in Windows you must make sure that network file sharing is enabled. Windows XP users should disable Simple File Sharing before proceeding. Windows Vista/7 users will find the option in the Sharing and Discovery section of the Network and Sharing Center. If you encounter any issues while enabling file sharing, please contact your IT administrator.
2. Open the *Properties* dialog for the case folder.
3. Click the **Sharing** tab to share the folder.
4. Edit the permissions on both the *Sharing* and *Security* tabs to allow the one authoritative user Full Control permissions.
5. Test connectivity to this share from the database system:
   5a. Open a Windows Explorer window on the system hosting the database.
   5b. Type *servername**sharename* in the address bar, where “servername” = the hostname of the Examiner host system, and “sharename” = the name of the share assigned in Step 1.
   For example: If the name of the system hosting the Examiner is ForensicTower1 and you named the share “FTK-Cases” in Step #1 above, the UNC path would be **\\forensictower1\FTK-Cases**.
   5c. Click **OK**. Check to see if the contents of the share can be viewed, and test the ability to create files and folders there as well.

Configure Database Services

To ensure access to all the necessary resources, the services upon which the database relies must be configured to log on as a user with sufficient permissions to access those resources.

To configure the database service(s) to Run As [service account]

1. On the database server system, open the Windows Services Management console:
   1a. Click **Start > Run**.
   1b. Type `services.msc`.
   1c. Press **Enter.**
2. Locate the following services:
   Oracle
   - Oracle TNS Listener service listed as `OracleFTK2TNSListener` or `OracleAccessDataDBTNSListener` (Found on Oracle System)
   - `OracleServiceFTK2` (Found on Oracle System)

   PostgreSQL
   - postgresql-x64-9.0
     or
   - postgresql-x86-9.0
3. Open the properties of the service and click the **Log On** tab.
4. Choose **This account**.
5. Click **Browse** to locate the service account username on the local system or domain. Ensure that “From this location” displays the appropriate setting for the user to be selected. Note that “Entire Directory” is used to search for a domain user account, while the name of your system will be listed for a workgroup system user.
6. In the object name box, type in the first few letters of the username and click **Check Names**. Highlight the desired username. Click **OK** when finished.
7. Enter the current password for this account and then enter it again in the *Confirm Password* box. Click **Apply** and then **OK**.
8. Repeat Steps #3-8 for each database service.
9. Restart database service(s) when finished.

Share the Backup Destination Folder

Using the same steps as when sharing the main case folder, share the backup destination folder. Use the UNC path to this share when performing backups. For a two-box backup to work correctly, you must use a single UNC path that both the examiner, and the database application have read/write access to.

Test the New Configuration

To test the new configuration

1. Launch the Case Manager and log in normally.
2. Select (highlight) the name of the case you want to backup.
   2a. Click **Case > Back up.**

2b. Select a back up destination folder.

Note: The path to the backup location must be formatted as a UNC path.

The *Data Processing* window opens, and when the progress bar turns green, the backup is complete. If the *Data Processing* window results in a red progress bar (sometimes accompanied by “Error 120”), the most likely cause is that the database service does not have permission to write to the backup location. Please double check all the steps listed in this document.

Chapter 46

AccessData Distributed Processing

Distributed Processing allows the installation of the Distributed Processing Engine (DPE) on additional computers in your network, allowing you to apply additional resources of up to three additional computers at a time to the processing of your cases.

Distributed Processing may not help reduce processing times unless the number of objects to be processed exceeds 1,000 times the number of cores. For example, on a system with eight cores, the additional distributed processing engine machines may not assist in the processing unless the evidence contains greater than 8,000 items.

This appendix includes the following topics

- See Distributed Processing Prerequisites on page 565.
- See Installing Distributed Processing on page 567.
- See Configuring Distributed Processing on page 569.
- See Using Distributed Processing on page 571.

Distributed Processing Prerequisites

Before installing the AccessData (AD) Distributed Processing Engine, the following prerequisites must be met (if you are not familiar with any one of these tasks, contact your IT administrator):

- The following software must be installed:
  - Evidence Processing Engine installed on the local examination machine.
  - CodeMeter Runtime software and either a USB or a Virtual CmStick. (For more information regarding the CmStick, see (page 542).)
  - Database either on the same computer, or on a second computer.
  - KFF Library.
  - McAfee Virus Scan must have an exception added for processes added to and run from the Temp Directory.
  - The Windows Temp directory must be set as default.
- A New user account that is a member of the Administrators group on the examiner machine. If you are installing on a Microsoft network with a Domain Controller, this is easily accomplished. If you are on a non-domain network or workgroup, create this same user account and password on each DPE machine, as well as on the machine holding the Case Folder and the machine holding the Evidence Folder.
  - Make a note of the user account, domain or workgroup, and the IP address of each machine.

- A familiarity with UNC paths. UNC paths are required whenever a path statement is needed during installation and configuration of the DPE, and when the path to the Case Folder, or the path to the Evidence Folder is required.
  - The UNC format is \\[*machine name or IP address*]\[*pathname*]\[*casefolder*].
- Computers that are all on the same network, and in the same domain or workgroup.
- A familiarity with the Windows **Services.msc** to ensure appropriate Login rights for the DPE, and for restarting the service, if necessary.
- A familiarity with IP addresses and how to find them on a computer.
- A knowledge of the case folder path. The case folder must be shared for DPE to access it and write to it as it processes case data.

Using PostgreSQL with Distributed Processing

- When using PostgreSQL, please note the following:
  - If the computer has fewer than 16 cores (< 16), then in the PostgreSQL configuration file, set the max_connections to 60 per computer.

    For example, if there are 4 computers in the Distributed Processing Model in which every computer has fewer than 16 cores, then set max_connections to 240 (60*4).
  - If the computer has 16 or more cores (>= 16), then in the PostgreSQL configuration file, set the max_connections to 125 per computer. For example, if there are 4 computers in the Distributed Processing Model in which 3 computers are 8 core (<16) and 1 computer is 16 core (>=16), then set max_connections to 245 (60*3 + 125*1).
  - If there is just one computer in the Distributed Processing Model, the max_connections should be no less than 100.

Installing Distributed Processing

Important: Do not install the Distributed Processing Engine on the examiner machine. The install required the installation of the local Evidence Processing Engine on that machine.

Installing the Distributed Processing Engine on the examination machine disables both processing engines.

Remedy: If you have already installed both the Evidence Processing Engine and the Distributed Processing Engine on a single machine, you must:

a) stop the processes

b) uninstall from both the examination machine and the Evidence Processing Engine machines

c) restart your machine

d) install on the examination machine.

e) start the Evidence Processing Engine again

To install AccessData Distributed Processing

1. Install the Distributed Processing Engine (AccessData Distributed Processing Engine.EXE) on the computers that are to participate in case processing, (record the IP address of each one for use when configuring the DPE on the examination machine).

   The DPE install file can be found on the installation disc in the following path:

   [*Drive*]:\FTK\AccessData Distributed Processing Engine.EXE

   If you do not know the IP address of the machine you are installing on, do the following:

   1a. Click **Start** on the Windows Startbar.

   1b. Click **Run**.

   1c. Enter cmd.EXE in the *Run* text box.

   1d. If the prompt is not **c:\>**, type **c:** and press **Enter**.

   At the new prompt, type **cd** and press **Enter**.

   The resulting prompt should be **c:\>**.

   1e. At the c:\> prompt, type **ipconfig /all.**

   1f. From the resulting information, locate the Ethernet adapter Local Area Connection, and find the associated IP address. That is what you will need when you configure the Distributed Processing Engine.

   Note: AccessData recommends that you write down the IP addresses for all machines on which the DPE will be installed.

   1g. At the prompt, type **exit** and press **Enter** to close the cmd.EXE box.

   Note: The domain listed here is not necessarily the correct one to use in installation. To find the correct domain or workgroup name, right-click **My Computer** (On Vista or Server 2008, click **Computer**), click **Properties** > **Computer Name**. The Domain or Workgroup name is listed midway down the page. Please make a note of it for future use.

2. If a *Security Warning* appears, click **Run** to continue.
3. If you want to stop the install, click **Cancel** on the Preparing to Install screen.
4. Click **Next** on the Welcome screen to continue the install.
5. Read and accept the License Agreement.

6. Click **Next** to continue.
7. Accept the default destination folder (recommended), or click **Change** to specify a different destination folder.
8. Click **Next** to continue.
9. Enter the credentials to be used for running the service.
   - *User name*: This user account must be a member of the Administrators group on the DPE machine, and must also have access to both the case folder, and the evidence folder. If this user account is not a member of the Administrators group, or if you are not sure, check with your IT services department.
   - While it is not generally necessary on a domain, it is recommended that whether you are on a domain network, a non-domain network, or a workgroup network, you create this same user account with the same password as a member of the Administrators group on all machines involved. This acts as a fail-safe in case the domain server goes down.
   - *Domain*: The name of the domain all related computers are on. If a non-domain or workgroup network is in place, use the local DPE's machine name or IP address in place of the domain name for this step in the installation.
   - *Password*: This user account's password for authenticating to the domain, or to the machine on the non-domain network or workgroup. The password must be the same for this user account on each machine.

   The figure below illustrates the user name and password setup.

   The components on the top row of the figure can be all on one machine, all on separate machines, or on any combination of machines. The key is that the administrator account and password (or user account in the Administrators group—it can be any name as long as the correct permissions are assigned, and the same name/password combination is used on each machine) must exist on all the machines related to the DPE installation, including the examination and database machines, and on both the Case Folder machine and on the Evidence Folder machine. This means physically going to those machines and adding the correct user accounts manually.
10. When you have finished adding the User Credentials, click **Next** to continue.
11. Click **Install** when the Ready to Install the Program screen appears.
12. Wait while the AccessData Distributed Processing Engine files are copied into the selected path on the local machine.
13. The default path is:

    [*Drive*]:\Program Files\AccessData\Distributed Processing Engine\<Version>.
14. Click **Finish** to complete the install and close the wizard.

If the service fails to start

1. Leave the *Retry/Quit* dialog open and launch the Services (**services.msc**) dialog from the run command.
2. Open the *Properties* dialog for the AccessData Processing Engine Service.
3. Click the **Log On** tab.
4. Verify that the logon credentials used have full Administrative rights.
5. Save the settings and exit the *Properties* dialog.
6. Stop and start the service manually.
7. Click **Retry** on the installer screen.

Configuring Distributed Processing

Once the AccessData Distributed Processing Engine is installed on the non-examination machines, configure Distributed Processing to work with the local Processing Engine.

To configure Distributed Processing to work with the local Lab Processing Engine

1. In *Case Manager*, click **Tools > Processing Engine Config**.
2. Enter the appropriate information in each field, according to the following guidelines:
   - *Computer Name/IP*: Enter the IP address of the computers where the Distributed Processing Engine is installed. The computer name can also be used if the name can be resolved.
   - *Port:* The default port is 34097. This is the port the processing host will use to communicate with the remote processing engines.
   - *Add*: Adds the computer and port to the list. You can add up to three remote processing engines (for a total of 4 engines). When the maximum number of DPE machines is reached, the Add button will become inactive.
   - *Remove*: Removes a processing engine from the list of available engines. The localhost engine cannot be removed.
   - *Enable*: Enables the engine for use by the processing host. Until implemented, each engine you add will be set to enabled (Disabled = False) by default. When implemented, you will be able to change the selected computer's status from Disabled to Enabled.
   - *Disable*: Makes the engine unavailable for use in processing. When implemented, you will be able to change the selected computer's status from Enabled to Disabled. The disabled remote engine will remain on the list, but will not be used.
   - *Disabled = True:* Displays for that engine in the DPE list.
   - *Maintain* UI *performance while processing*: Allows you to decide whether processing speed or UI performance is more important.

   Note: This will slow processing, and when selected, applies to *all* Remote DPEs.

3. When all DPE machines have been added to the Processing Engine Configuration dialog, click **Close**.

If you have not yet configured the Distributed Processing Engine on the remote computers, or if you have, but it is not working properly, you will see the warning shown in the following figure.

To correct this

1. On the remote computer having the Distributed Processing Engine installed, click **Start**.
   1a. Right-click **My Computer.**
   1b. Click **Manage.**
   1c. Under *System Tools*, click **Local Users and Groups.**
   1d. Click **Groups**.
   1e. Double-click **Administrators.**
   1f. Verify that the user account name that was used in installation is in this group.
   1g. Click **OK** to close this dialog.
2. Under Local Users and Groups, click **Users.**
   2a. Find the user account name in the list, and double-click it.
   2b. Mark the box **User cannot change password**.
   2c. Mark the box **Password never expires**.

2d. Click **Apply**.

2e. Click **OK.**

3. Do one of the following:

   - Under Services and Applications, click **Services**.
   - If you already closed the Computer Management dialog, launch the Services (**services.msc**) dialog from the Run command on the Start menu.

   3a. Open the Properties dialog for the AccessData Processing Engine Service.

   3b. In the General tab, find Startup Type. If it says Automatic, proceed to the next step. If it says anything else, click the drop-down on the right side of the text box and select Automatic from the list. Click **Apply** and proceed to the next step.

   3c. Open the *Log On* tab.

   3d. Verify that the *Log On information* is set to the user name, domain or DPE machine name, and password that matches the user account you just verified (should be the one that was entered during installation).

   3e. Click **OK**.

4. Right-click on the *AccessData Processing Engine Service.*
5. Click **Stop** to stop the service.
6. Click **Start** to re-start the service manually.
7. Click **Retry** on the installer screen.
8. Ensure that the user name provided during installation is a member of the Administrators account.

Using Distributed Processing

To utilize the Distributed Processing Engine when adding evidence to a case

1. Make sure the case folder is shared before trying to add and process evidence.
2. Enter the path to the case folder in the *Create New Case* dialog in UNC format.
3. Click **Detailed Options**, and select options as you normally would.
4. Click **OK** to return to the *New Case Options* dialog.
5. Mark **Open the case** and then click **OK** to create the new case and open it.
6. The new case is opened and the *Manage Evidence* dialog is automatically opened. Click **Add**. Select the evidence type to add. Select the evidence file to add and then click **Open**.
7. The path to the evidence is designated by drive letter by default. Change the path to UNC format by changing the drive letter to the machine name or IP address where the evidence file is located, according to the following syntax:

   \\[*computername_or_IP_address*]\[*pathname*]\[*filename*]
8. Leave the remaining path as is.
9. Click **OK**.

Note: If a case was originally processed using distributed processing, when a reviewer conducts a live search, the system will first attempt to use the computer with the distributed processing engine, but if it is not available, it will use the reviewer's local computer to conduct the search.

Checking the Installation

When you have completed the installation, open the Task Manager on the remote computer, and keep it open while you add the evidence and begin processing. This will allow you to watch the activity of the ProcessingEngine.EXE in the Processes tab.

The Distributed Processing Engine does not activate until a case exceeds approximately 30,000 items. When it does activate, you will see the CPU percentage and Memory usage increase for the ProcessingEngine.EXE in Task Manager.

Chapter 47

AccessData Oradjuster

AccessData **Oradjuster.EXE** optimizes certain settings within an AccessData Oracle database, and this allows peak performance during investigative analysis to be obtained. This utility is particularly useful for 64-bit systems with large amounts of RAM on board. It is included in the AD Lab Database install disc.

This document describes Oradjuster's role in making maximum use of AD Oracle. To see a webinar that demonstrates Oradjuster, look under the Core Forensic Analysis portion of the web page: http://www.accessdata.com/Webinars.html.

This chapter includes the following topics

- See Oradjuster System Requirements on page 572.
- See Introduction on page 572.
- See The First Invocation on page 573.
- See Tuning for Large Memory Systems on page 576.

Oradjuster System Requirements

Oradjuster operates on all supported Windows platforms (both 32 and 64-bit) where and AD Oracle database has been installed.

Introduction

The Oracle database system's behavior is governed, in part, by its numerous Initialization Parameters, which define many internal database settings. Oradjuster is concerned with two small groups of these parameters. The first group regulates the memory usage of **oracle.EXE**, and the second group controls the number of client programs that can be connected simultaneously to the database.

Although Oradjuster is not mandatory, it is very helpful. For many investigators, it is ideal to run Oradjuster immediately following the AD Oracle install by clicking the *Optimize the Database* button on the Database installation autorun menu. Later on, Oradjuster can be invoked again (one or more times) in order to fluctuate database memory usage and derive even greater performance gains throughout the several phases of an investigation.

The First Invocation

When Oradjuster is invoked for the first time, it does the following

1. Detect AD Oracle.
2. Query Windows to discover the size of RAM.
3. If necessary, prompt for the database's administrative password.
4. Display the current values of the parameters of interest.
5. Compute new values (based on the size of RAM) and modify the parameters with them.
6. Shut down and restart the database.
7. Display the updated parameter values.
8. Record the new values in a Windows Registry key.

Some of these steps will be treated in greater detail in what follows.

Note: When Oradjuster is invoked from the install autorun menu, it does not linger on screen. It disappears as soon as it has completed successfully, which is done in deference to those who may not take an interest in its esoteric display information.

Oradjuster's first invocation brings great improvement to performance, and many investigators may find this satisfactory. However, as mentioned previously, subsequent use of Oradjuster can yield additional performance improvements.

Subsequent Invocations

The use case scenarios described in this section illustrate how to employ Oradjuster to greatest effect in configurations knows as One-Box and Two-Box.

Note: Some of the instructions below describe the invocation of Oradjuster from the command prompt. Working from the command prompt may be a foreign experience for many, but any time/effort spent becoming familiar with the command prompt and command line programs is worthwhile because it facilitates advanced use of Oradjuster, and it opens a door to the large number of valuable and intriguing command line programs available (serving many diverse purposes, including digital forensics).

One-Box Deployment

Oradjuster's default behavior is to assume that the *Examiner* and the database are installed on the same computer. The settings it applies on its first run strikes a balance between the memory needs of *Examiner*, AD Oracle, and the operating system. Additional performance gains can be won by reducing `oracle.EXE` memory consumption during evidence processing and then increasing `oracle.EXE`'s memory consumption during investigative analysis after automatic processing has completed.

To accomplish this fluctuating of oracle.EXE memory usage

1. After creating a case, but before adding and processing evidence, launch Oradjuster from the *Case Manager*'s Tools menu.
2. Oradjuster will display its normal output and then prompt the user to make a temporary change to SGA_TARGET (one of the Oracle database parameters having direct impact on memory consumption). The value for SGA_TARGET is specified as a percentage of the size of physical memory, and the allowable range is typically between 10% and 50%. Enter a percentage in the lower half of the allowed range.
3. Add and process the case's evidence.
4. After processing is complete, launch Oradjuster again from the *Case Manager*'s *Tools* menu.
5. Modify SGA_TARGET to a percentage in the upper half of the allowed range.
6. Complete the investigation of the case without modifying SGA_TARGET again unless more evidence is added and processed.

Some trial-and-error experimenting is required to find the most optimal percentages. For example, it may be desirable to set SGA_TARGET to the maximum allowable percentage in Step 5, rather than just some percentage in the upper half of the range, so that the case window is most responsive. Also, it may be good to reduce SGA_TARGET during Live searching (in spite of Step 6) as Live searching is similar in nature to evidence processing.

Two-Box Deployment

When *Examiner* is installed on computer A, and AD Oracle is installed on computer B, oracle.EXE should be even more aggressive in consuming memory on computer B since it does not need to share memory resources with the *Examiner*. The following procedure should be conducted.

To begin, log in to computer B.

Note: If Oradjuster has been run on this computer before (as part of AD Oracle install and setup), then its Registry key must be deleted before proceeding. Select **Start Menu** > **Run**. Enter "regedit" in the Run prompt and press **Enter**. Within the Registry Editor dialog, navigate to and delete the following key:

HKEY_LOCAL_MACHINE\Software\AccessData\Shared\Version Manager\sds\oradjuster

Important: Do not delete or modify any other Registry keys or your system may become unstable.

Open the command prompt (select **Start Menu > All Programs > Accessories > Command Prompt**). Then, issue the following commands (press the **Enter** key after each one):

Oradjuster Command Line Options

Command	Explanation
C:\> cd "Program Files\AccessData\ Oracle\Oradjuster"	Move to the directory containing Oradjsuter.EXE. On a 64-bit version of Windows, the directory path should be "Program Files(x86)\AccessData\Oracle\Oradjuster".
C:\[path]> Oradjuster.EXE -mem remoteworker	Assign parameter values appropriate for a dedicated AD Oracle database.

As with Step 6 in section The First Invocation, and the database will be restarted. Some of the Oracle parameters managed by Oradjuster cannot be modified “on the fly,” so the database must be restarted in order for their changes to take effect. Therefore, when invoking Oradjuster from the command prompt, first close the *Examiner* (by closing all case windows and the case management window).

Tuning for Large Memory Systems

When AD Oracle resides on a computer with a 64-bit Windows operating system, and with a large quantity of RAM (from 8 GB to 128 GB, or higher), additional considerations are in order. As was hinted in section One-Box Deployment, Oradjuster's first run assigns oracle.EXE's maximum memory consumption to roughly ½ the size of RAM. (That is why the upper limit for SGA_TARGET is typically 50%.) Instead of sharing memory proportionally between AD Oracle and the operating system, Oradjuster can be used to give oracle.EXE the lion's share of memory, which would not be safe on a computer with a lesser quantity of RAM. This is best accomplished by editing Oradjuster's key in the Registry and then running Oradjuster again, which causes Oradjuster to apply the new, manually-entered values in the Registry key to AD Oracle.

Consider an investigative computer with 64 GB of RAM that hosts AD Oracle and the *Examiner*. Suppose that the investigator ran Oradjuster in conjunction with the AD Oracle install, and has since conducted several large cases (containing millions of discovered items each). The investigator is generally content with the case window's responsiveness in loading and sorting its File List pane, but wonders if that responsiveness could be improved. So, she prepares to edit the **SGA_MAX_SIZE** and **SGA_TARGET** values in the Oradjuster key in the Registry. When she opens Registry Editor and first navigates to the key, she sees that current values read:

Example of Oradjuster Settings

Name	Type	Data
...	...	...
sga_max_size	REG_SZ	37795712204
sga-target	REG_SZ	13743895347
...	...	...

These values represent quantities expressed in Bytes, and therefore the investigator can see that Oradjuster has set **SGA_MAX_SIZE** to about 37 GB, and **SGA_TARGET** value of roughly 13 GB. She knows that she can temporarily alter the value of **SGA_TARGET** using the technique shown in One-Box Deployment, but she can only increase it to the upper limit imposed by **SGA_MAX_SIZE**. So, she decides to make the following edits:

Example of User-Modified Oradjuster Settings

Name	Type	Data
...	...	...
sga_max_size	REG_SZ	*48*795712204
sga-target	REG_SZ	*32*743895347
...	...	...

By modifying only the first two digits of Data field for each value, the investigator has paved the way for Oradjuster to make the desired change to AD Oracle. (If she had wanted, the investigator could have edited the Data field to contain a number that would be easier to read, such as "48000000000," but the net effect would be the same. And, the smaller the edit, the less chance of loosing a digit or inserting an extra one, both of which may require a troubleshooting effort to repair.) As soon as Oradjuster is again invoked, the new upper limit for

oracle.EXE memory usage will be approximately 48 GB (a jump from about ½ to about ¾ of RAM), and SGA_TARGET will be set to about ½ of RAM by default.

The investigator closes the *Examiner* (knowing that her edit of SGA_MAX_SIZE in the Registry will cause Oradjuster to restart AD Oracle) and runs Oradjuster again. (In this context, she can do so either by invoking it from the command prompt, or by launching it with a double-click.) When Oradjuster completes its assignment changes, and prompts the investigator to make a temporary change to SGA_TARGET if desired, she pauses to review the before and after values in the Oradjuster output to confirm that the changes to SGA_MAX_SIZE and SGA_TARGET are correct.

Note: When Oradjuster assigns a new value to SGA_MAX_SIZE, oracle.EXE will modify it rounding it up the nearest multiple of 16 MB. Therefore, when inspecting Oradjuster output, remember to confirm that the first (or left-most) digits of SGA_MAX_SIZE are correct. Do not be alarmed if trailing digits have been altered.

Finally, the investigator creates several more large cases with her new settings. She observes that the case window is in fact more responsive and she pays attention to evidence processing times to see whether or not oracle.EXE's increased claim on system memory appears to slow down evidence processing...

In conclusion, and although the vast majority of tuning needs have been addressed by the preceding information, additional explanation will allow a curious investigator to go even further in using Oradjuster.

First, the list of supported command line arguments can be displayed with the command:

```
C:\[path]> Oradjuster.exe -help
```

Second, the following table provides a listing of the values Oradjuster records in its Registry key.

Oradjuster Values Found in its Registry Key

Value Name	Provokes DB Restart	Type
_pga_max_size	NO	Memory Usage
_smm_max_size	NO	Memory Usage
commit_write	NO	Memory Usage
open_cursors	NO	Memory Usage
pga_aggregate_target	NO	Memory Usage
processes	YES	Number of Concurrent Connections
session_cached_cursors	YES	Memory Usage
sessions	YES	Number of Concurrent Connections
sga_max_size	YES	Memory Usage
sga_target	NO	Memory Usage
Transactions	YES	Number of Concurrent Connections
VERSION	N/A	Oradjuster Version Information — Do not edit